Verwaltungsakademie Berlin
Anstalt des öffentlichen Rechts

Berlin

Lehrbrief Informationstechnik

Ausgabe 2011

Autor: Karsten Fecke

L E H R B R I E F

1. Ausgabe

Erarbeitet von: Karsten Heinlein (2000)

2. überarbeitete Ausgabe

Überarbeitet von: Karsten Fecke (2008)

3. überarbeitete Ausgabe

Überarbeitet von: Karsten Fecke (2011)

Änderungsdienst

Der Lehrbrief unterliegt einer ständigen Anpassung an neue Entwicklungen aus Politik, Wirtschaft und Verwaltung. Wünsche, Anregungen, Ergänzungen und Verbesserungsvorschläge zu diesem Lehrbrief richten Sie bitte an die

Verwaltungsakademie Berlin
- Ausbildungszentrum -
Alt-Friedrichsfelde 60
10315 Berlin

© Verwaltungsakademie Berlin

Nachdruck sowie jede Art von Vervielfältigung und Weitergabe nur mit Genehmigung der Verwaltungsakademie Berlin.

Inhaltsverzeichnis

1. Einführung....6

2. Geschichtliche Grundlagen....8

2.1. Epochen der Entwicklungsgeschichte....8
2.2. Personen der Zeitgeschichte....10
2.2.1. Hermann Hollerith....10
2.2.2. Konrad Ernst Otto Zuse....11

3. Allgemeine Grundlagen....14

3.1. IT-Grundrecht....14
3.2. Gründe für die Anwendung der Informationstechnik....15
3.3. Entwicklung....15
3.4. Ziele des Einsatzes der Informationstechnik....17
3.4.1. Aktuell....17
3.4.2. Schnell....17
3.4.3. Im benötigten Umfang....17
3.4.4. Wirtschaftlich....17
3.4.5. Verfügbarkeit zum richtigen Zeitpunkt....18
3.5. Auswirkung auf das Verwaltungshandeln....18
3.6. Grenzen der Automatisierbarkeit in der Verwaltung....18
3.7. Die Informationstechnik....20
3.8. Informationsarten....21
3.8.1. Texte und Zahlen....21
3.8.2. Logogramme/Pictogramme....22
3.8.3. Grafik....23
3.8.4. Foto/Video....23
3.8.5. Sprache....24
3.8.6. Signale, Messwerte....25
3.9. Digitale und analoge Daten 25
3.10. Erfassen, Verarbeiten und Ausgeben von Informationen....28

4. Aufbau der Informationstechnik....33

4.1. Hardware....33
4.1.1. Eingabegeräte....34
4.1.2. Verarbeitungsgeräte....44
4.1.3. Ausgabegeräte....46
4.1.4. Speichergeräte / Datenträger....53
4.2. Software....58
4.2.1. Betriebssystem....58
4.3. Anwendungssoftware....62
4.3.1. Textverarbeitung....62
4.3.2. Textmengenorientierte Funktionen....63
4.3.3. Dokumentbezogene Funktionen....64
4.3.4. Tabellenkalkulation....65
4.3.5. Datenbank....66
4.4. Open Source Software....68
4.4.1. Beispiele für Open Source-Software....69
4.5. Benutzeroberfläche....70

5. Netze und Postdienste....73

5.1. PC-Netzwerke....73

5.1.1. Technische Komponenten 74
5.1.2. Vorteile eines PC-Netzwerkes (Rechnerverbundsystem) 74
5.1.3. Netzwerkbetriebssystem 75
5.1.4. Standardsoftware für Netzwerke 75
5.1.5. Benutzung des Netzwerkes 76
5.1.6. Rollen 76
5.2. Netzwerktypen 76
5.2.1. LAN (Local Area Network) 77
5.2.2. WLAN (Wireless Local Area Network) 77
5.2.3. VLAN (Virtual LAN) 77
5.2.4. MAN (Metropolitan Area Network) 78
5.2.5. WAN (Wide Area Network) 78
5.2.6. GAN (Global Area Network) 78
5.3. Bestandteile eines Netzwerkes 79
5.3.1. File-Server = Datenserver 79
5.3.2. Workstation 79
5.3.3. Netzwerkkarten 79
5.3.4. Netzwerk-Kabel 80
5.4. Internet 80
5.5. Intranet 81
5.6. Barrierefreiheit 82
5.6.1. Barrierefreies Internet/Intranet 82
5.6.2. Grundlegende Techniken für ein barrierefreies Internet 84

6. Umgang mit Anwendungen der Informationstechnik 88

6.1. Einführung in die Gerätebedienung 88
6.1.1. Windows-Explorer 88
6.1.2. Dateipfad 89
6.1.3. Ordnerstruktur 89
6.1.4. Begriff “Datei” 89
6.1.5. Dialogfeld 91
6.1.6. Klicken 91

7. Organisatorische und rechtliche Regelungen 95

7.1. Tarifvertrag Infotechnik 95
7.1.1. Geltungsbereich 95
7.1.2. Begriffsbestimmungen 95
7.1.3. Zusammenarbeit mit dem Personalrat 97
7.1.4. Ausstattung der Arbeitsplätze 98
7.1.5. Schutzbestimmungen 99
7.2. Weitere Rechtsvorschriften 102
7.3. Arbeitsplatzgestaltung 102
7.3.1. Ergonomie 102
7.3.2. Arbeitsmöbel 107

8. Datenschutz und Datensicherheit 110

8.1. Datenschutz 110
8.1.1. Was soll Datenschutz bewirken? 110
8.1.2. Die Entwicklung des Datenschutzes 111
8.1.3. Begriffsbestimmungen 114
8.1.4. Prinzip des Datenschutzes 115
8.1.5. Kontrollmöglichkeiten 116
8.1.6. Technisch-organisatorische Maßnahmen 119
8.2. Datensicherheit (IT-Sicherheit) 122
8.2.1. Definition 122
8.2.2. Möglichkeiten der Sicherung 123

8.2.3. Unterscheidung Einzelplatz / Netz....126
8.2.4. Leitsätze zur IT-Sicherheit....126
8.2.5. Viren128
8.2.6. Phishing....131
8.2.7. Spam....132
8.2.8. Falschmeldungen....133

9. New Public Management....134

9.1. Inhalt und Ziele....134
9.2. Theoretisch-konzeptioneller Hintergrund....135
9.3. Kritik 136
9.4. Neues Steuerungsmodell....136
9.4.1. Begriff und Inhalte....136
9.4.2. Ausgangssituation und Geschichte....137
9.4.3. Erläuterung der Elemente....138
9.4.4. Bewertung....140

10. E-Government....142

10.1.1. Beziehungen....145
10.1.2. Verfahrenssicherheit....145
10.2. E-Commerce....146
10.3. E-Learning....148
10.3.1. Blended Learning....148
10.3.2. Web Based Training....149
10.4. Elektronische Signatur....149
10.4.1. Formen der elektronischen Signatur....150
10.5. Voice over IP....151
10.6. Telearbeit....152

11. Auswirkungen der Informationstechnik....155

11.1. IT-Regelwerk....156
11.2. IT-Organisationsgrundsätze....157
11.3. Cloud Computing....158
11.3.1. Architektur....159
11.3.2. Arten von Clouds....160

Anhang 1: Bundesdatenschutzgesetz....162

Anhang 2: Berliner Datenschutzgesetz....190

Anhang 3: Informationsfreiheitsgesetz....205

Anhang 4: Die bekanntesten Betriebssysteme....208

Anhang 5: Die Betriebssysteme der Firma Microsoft....210

Anhang: 6 Einen Serienbrief erstellen....212

Anhang 7: Netzwerktopologien....216

Anhang 8: Literatur- und Quellenangaben....220

Anhang 9: Probeklausur....221

Anhang 10: Lehrpläne....224

1. Einführung

In allen Bereichen des täglichen Lebens, im Beruf wie im Privatleben werden Informationen gesammelt, bearbeitet und aufbewahrt. Die dafür eingesetzten technischen Hilfsmittel haben sich im Laufe der Jahre stark verändert.

Ein besonders kräftiger Impuls für die Veränderung von Arbeitsabläufen und Arbeitsumgebungen ging von dem Erfolg des PERSONAL COMPUTER (PC) seit Anfang der 80er Jahre aus. Bereits frühzeitig umfassend in der freien Wirtschaft eingesetzt, sind die PERSONAL COMPUTER (PC) heute auch in der Verwaltung nicht mehr weg zu denken. Ihre Verwendung ist für viele Bereiche der Verwaltung unverzichtbar geworden und ihre Einsatzbereiche werden sich weiter ausdehnen. Neue Techniken werden in die Verwaltungsarbeit mit einbezogen.

Will man die Leistungsfähigkeit der PERSONAL COMPUTER (PC) umfassend nutzen, muss man auch über ihre Bedienung und über ihre Einsatzmöglichkeiten informiert sein.

Von den Beschäftigten der Verwaltung werden daher unabdingbar Kenntnisse in den Grundlagen und in der Anwendung der Informationstechnik verlangt. Diese Grundlagen sind wichtig für die Nutzung und Bedienung teilweise spezieller Fachsoftware in den Berliner Verwaltungszweigen. Dieser Lehrbrief soll Ihnen die Möglichkeit geben, entweder als reiner „Trockenkurs“ oder aber im praktischen Teil durch Arbeit am PERSONAL COMPUTER (PC), diese Grundlagen zu erwerben.

Am Anfang jedes Themenbereichs werden Sie über die Lernziele dieses Bereichs informiert. Außerdem haben Sie die Möglichkeit Ihren persönlichen Lernerfolg durch die Beantwortung von Kontrollfragen am Ende eines jeden Abschnitts zu überprüfen.

Die Testfragen nach größeren Abschnitten sollen es Ihnen ermöglichen, Lerninhalte zu festigen und das gelernte Wissen anzuwenden. Mit Hilfe dieses Lehrbriefes sollen keine vertieften Kenntnisse im Umgang mit Fachanwendungen vermittelt werden. Im Laufe der Unterrichtsveranstaltung werden jedoch praxisbezogene Übungen mit den Standard-Office-Anwendungen der Berliner Verwaltung durchgeführt.

Sie sollen hierdurch einen ersten Einblick in die Möglichkeiten der Einzelanwendungen erhalten. Vielleicht kann bei Ihnen durch den umfassenden und teilweise auch über das Grundlagenwissen hinausgehenden Inhalt dieses Lehrbriefes auch das Interesse an der Informationstechnik geweckt werden.

Das Ausbildungszentrum der Verwaltungsakademie Berlin bietet Ihnen im Rahmen der dienstlichen Fortbildung spezielle Kurse zu diesen Fachanwendungen an.

Und nun viel Spaß und viel Erfolg!

Genderhinweis:

Alle Personen- und Aufgabenbezeichnungen sind mit Rücksicht auf die Lesbarkeit des Dokumentes weitgehend geschlechtsneutral oder – wo dies seinerseits zu einem missverständlichen Text geführt hätte – in der (fach-)umgangssprachlichen Form gewählt worden. Unabhängig von der gewählten Bezeichnung können alle genannten Personen- und Aufgabenbezeichnungen gleichermaßen von Frauen oder Männern wahrgenommen werden.

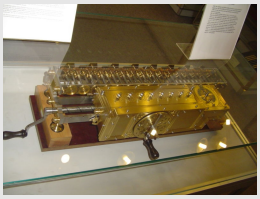
2. Geschichtliche Grundlagen

Lernziele:

Der/Die Lernende soll ohne Hilfsmittel und mit eigenen Worten:

- die wichtigsten Epochen der Entwicklung wiedergeben können
- die Personen der Zeitgeschichte kennen

2.1. Epochen der Entwicklungsgeschichte

1100 v. Chr.	**Der Abakus**
	Der Abakus besteht aus einem Rahmen mit Kugeln oder Steinen (auch als Calculi bezeichnet), die auf Stäben aufgefädelt bzw. in Nuten, Rillen oder Schlitzen geführt werden.
1617	Die Rechenstäbchen von John Napier Laird of Merchiston
	Bei den Stäbchen handelte es sich um längliche, etwa 6 cm lange Stäbchen aus Holz oder Plastik, welche in verschiedenen Farbtönen eingefärbt waren.
1622	Der Rechenschieber von William Oughtred
	Ein Rechenschieber oder Rechenstab ist ein analoges Rechenhilfsmittel zur mechanisch-optischen Durchführung von Grundrechenarten wie Multiplikation und Division.
1623	Die Rechenmaschine von Wilhelm Schickard
	Eine Rechenmaschine ist eine Maschine, mit deren Hilfe bestimmte mathematische Berechnungen automatisiert ausgeführt werden können.
1641	Die Addiermaschine von Blaise Pascal 
1673	Die Rechenmaschine von Gottfried Wilhelm Leibniz

1805	Die Lochkarte von Joseph-Marie Jacquard
1833	Die analytische Maschine von Charles Babbage
1886	Die Lochkartenmaschine von Hermann Hollerith
1934 – 1943	Der erste funktionsfähige Computer Zuse 3 von Konrad Zuse
1934 – 1944	Mark I von Howard H. Aiken
1946 – 1952	Die Neumann-Maschine von John von Neumann
1946	Der Eniac von John P. Eckert und John W. Mauchly
	Der Electronic Numerical Integrator and Calculator (ENIAC) war der erste rein elektronische digitale Universalrechner. Im Auftrag der US-Armee wurde er ab 1942 an der University of Pennsylvania entwickelt und am 14. Februar 1946 der Öffentlichkeit vorgestellt. Bis zu seiner Abschaltung am 2. Oktober 1955 diente er der US-Armee zur Berechnung ballistischer Tabellen
1955 – 1960	Der Tradiac von J.H. Felker
1962 – 1970	Die integrierten Schaltkreise
1968	Die hoch integrierten Schaltkreise
1974	Die ersten Heimcomputer
1977	Der erste Apple-Computer
1980	Der Cray-Computer
1981	Der erste IBM-Personalcomputer
1987	Der Apple Macintosh
seit 1985	die Vernetzung von Computern
1989	Das Betriebssystem OS/2 von IBM
1991/1992	Wechsel von MS-DOS zu Windows 3.0/3.1
1993	Erscheinen des ersten Pentium-Prozessors der Firma Intel
1995	Windows 95 wird von der Firma Microsoft auf den Markt gebracht
1998	Die Suchmaschine Google geht am 7. September als Testversion online.

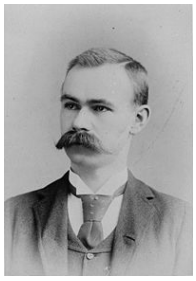
2000	Windows 2000 wird vorgestellt; die Firma Apple bringt fast zeitgleich das bis heute aktuelle Betriebssystem Mac OS X auf den Markt.
2001	Das Betriebssystem Windows XP erscheint im September, kurz danach wird der erste iPod der Firma Apple verkauft. Gleichzeitig wird der legale Download von Musik aus dem Internet revolutioniert.
2006	Für Firmenkunden verkauft Microsoft ab November das Betriebssystem Windows Vista; für Privatkunden startet der Verkauf zu Beginn des Jahres 2007

2.2. Personen der Zeitgeschichte

Die Geschichte der elektronischen Datenverarbeitung ist nun bereits über 50 Jahre alt. Nur wenige andere technische Entwicklungen beeinflussen unser tägliches Leben so stark. Ohne dass Sie ein besonderer Fan dieser Technik sein müssen, haben Computer bereits heute an vielen Orten des täglichen Lebens einen nicht zu übersehenden Einfluss auf unseren Alltag.

Stellvertretend für viele andere Personen der Zeitgeschichte, die an der Entwicklung der heutigen Computer beteiligt waren, werden nachfolgend zwei Personen näher aufgeführt:

2.2.1. Hermann Hollerith



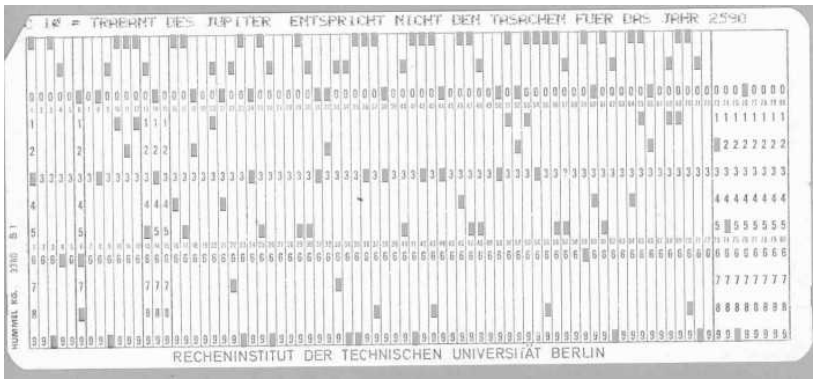
Herman Hollerith (* 29. Februar 1860 in Buffalo, New York; † 17. November 1929 in Washington, D.C.) war ein US-amerikanischer Unternehmer und Ingenieur. Er ist Erfinder des nach ihm benannten Hollerith-Lochkartenverfahrens in der Datenverarbeitung. Hollerith wurde im US-Bundesstaat New York als Kind deutscher Einwanderer aus Großfischlingen in der Pfalz geboren.

Er studierte an der Columbia University Ingenieurwissenschaften. Als studierter Bergbauingenieur hatte er Patente für eine automatische Eisenbahn-Druckluftbremse und für die maschinelle Herstellung von Wellblechplatten angemeldet.

Da er zunächst als Statistiker für die US-amerikanische Regierung arbeitete, beschäftigte er sich mit der Erfassung und Speicherung von Daten mittels Lochkarten. Dabei griff er auf die Konstruktionsideen des französischen Mechanikers Falcon zurück, der seinen Webstuhl mittels eines Holzbrettchens mit Lochkombinationen steuerte und der Weiterentwicklung dieses Verfahrens durch Jacquard, der das Holzbrettchen durch Lochkarten aus Pappschablonen ersetzte, übertrug Hollerith das Steuerungsverfahren mittels gelochter Karten auf organisatorische Problemstellungen. Als Vorbild verwandte er ein zur

damaligen Zeit im Eisenbahnbereich gebräuchliches System, das mittels mehrerer Löcher in den Fahrkarten die Fahrgäste nach Geschlecht und Alter klassifizierte. Er entwickelte ein System zur Erfassung von Daten auf Lochkarten. Am 9. Dezember 1888 installierte er die Erfindung im US-Kriegsministerium. Am 8. Januar 1889 meldete er sein System zum Patent an.

Sein System wurde bei der Volkszählung 1890/1891 verwendet (Hollerithmaschine genannt). Es trug zu einer enormen Beschleunigung der Auszählung bei. Es wurde möglich, diese in nur zwei Jahren mit 43 Maschinen und 500 Leuten als Bedienungspersonal auszuwerten, zuvor hätte dieselbe Anzahl an Leuten ganze sieben Jahre gebraucht.


1# = TRABANT DES JUPITER ENTSPRICHT NICHT DEN TASACHEN FUER DAS JAHR 2590
RECHENINSTITUT DER TECHNISCHEN UNIVERSITÄT BERLIN

Von zentraler Bedeutung war auch, dass die Maschinen nicht verkauft, sondern nur vermietet wurden. Holleriths erster größerer Auftrag außerhalb der Vereinigten Staaten kam aus Russland, wo erstmals eine Volkszählung durchgeführt wurde.

Nach weiteren Verbesserungen des Systems gründete er schließlich 1896 die Tabulating Machine Company, um seine Erfindung kommerziell zu verwerten. Allerdings verlor er 1905 aufgrund überzogener Preise seinen besten Kunden, das US-amerikanische Census Bureau, welches bis heute alle zehn Jahre Volkszählungen durchführt. Er verklagte 1910 erfolglos das Bundesbüro zur Durchführung von Volkszählungen wegen angeblicher Patentverletzung und versuchte so die Volkszählung zu verhindern. 1911 verkaufte Hollerith schließlich seine Gesellschaft für rund 1,21 Millionen Dollar plus einen über zehn Jahre laufenden Beratervertrag, der mit 20.000 Dollar jährlich dotiert war. Tabulating Machine Company fusionierte mit der Computing Scale Corporation und der International Time Recording Company zur Computing Tabulating Recording Corporation (CTR). 1924 wurde CTR schließlich in International Business Machines Corporation (IBM) umbenannt.

2.2.2. Konrad Ernst Otto Zuse

Konrad Ernst Otto Zuse (* 22. Juni 1910 in Berlin; † 18. Dezember 1995 in Hünfeld bei Fulda

Er war ein deutscher Bauingenieur, Erfinder und Unternehmer (Zuse KG). Mit seiner Entwicklung des Z3 im Jahre 1941 gilt er als der Erfinder des Computers.

Insgesamt hatte Zuse acht Ehrendoktortitel und zwei Ehrenprofessuren.

Nach ihm sind zwei Medaillen benannt, die zum einen von der Gesellschaft für Informatik und zum anderen vom Zentralverband des Deutschen Baugewerbes für besondere Leistungen auf dem Gebiet der Informatik vergeben werden.

1941 baute er in einer kleinen Wohnung in der Kreuzberger Methfesselstraße den Z3. Es war ein vollautomatischer in binärer Gleitkommarechnung arbeitender Rechner mit Speicher und einer Zentralrecheneinheit aus Telefonrelais. Berechnungen konnten programmiert werden, jedoch waren keine bedingten Sprünge und Programmschleifen möglich. Die Z3 gilt heute als erster funktionstüchtiger Computer der Welt.

Der Zweite Weltkrieg machte es ihm unmöglich, mit Rechnerspezialisten in Großbritannien und den USA in Kontakt zu treten. Die Z3 war an der Grenze, den theoretischen Anforderungen der Turingmaschine zu genügen. Der Beweis wurde erst viel später (1998) durchgeführt.

Zuses Berliner Unternehmen wurde 1945 durch einen Bombenvolltreffer zusammen mit der Z3 zerstört. Die teilweise fertig gestellte Z4 war vorher von Konrad Zuse und seinen Mitarbeitern zerlegt und in mehrere Kisten verpackt worden. Mit einem Militär-Lkw wurden die Kisten nach Süddeutschland in Sicherheit gebracht. Zuerst kam Zuse in Oberjoch, im Sporthotel „Ingeburg“, dem heutigen Alpenhotel unter. Hier lernte er den legendären Pionier der Raumfahrt, Werner von Braun, kennen. Später wurden die Kisten mit der Z4 nach Hinterstein verbracht und im Gasthaus Steinadler sowie in der Turnhalle vor dem Zugriff der Alliierten versteckt. Zuse entwickelte in der Zeit von 1941-1945 den Plankalkül, der als die erste universelle Programmiersprache der Welt gilt. Allerdings konnte sie auf den damaligen Computern noch nicht implementiert werden; das gelang erst im Jahr 2000.

Nach dem Krieg gründete Zuse 1949 in Neukirchen im damaligen Kreis Hünfeld die Zuse KG. Die Z4 wurde fertig gestellt und an der Eidgenössischen Technischen Hochschule (ETH) Zürich installiert. Zu jener Zeit war das der einzige funktionierende Computer in Europa und der erste kommerzielle Computer weltweit. Die Z4 wurde einige Monate früher als die UNIVAC installiert.

Weitere Computer wurden gebaut, die Typenbezeichnung war immer ein Z und eine fortlaufende Nummer. Herausragend war die Z11, die der optischen Industrie und Universitäten verkauft wurde, und die Z22, der erste Computer mit Magnetspeicher.

1957 wurde der Firmensitz von Neukirchen nach Bad Hersfeld verlegt. Bis 1967 baute die Firma insgesamt 251 Computer. Ab 1964 stieg Zuse als aktiver Teilhaber aus der Firma aus, sie wurde zun-

ächst von der deutschen BBC in Mannheim, Anfang 1967 dann von Siemens übernommen. Zuse erhielt für seine Arbeit mehrfach Auszeichnungen. 1981 wurde ihm die Ehrendoktorwürde der Technischen Universität Dresden verliehen. Nach seiner Pensionierung widmete er sich seinem Hobby, der Malerei. Unter dem Pseudonym „Kuno See“ schuf er abstrakte Bilder und Portraits berühmter Zeitgenossen. Auf der CeBIT in Hannover 1995 überreichte er Bill Gates ein selbst gemaltes Portrait von ihm. 1969 schrieb Zuse das Buch Rechnender Raum (Details siehe unter Werke). Darin entwickelte er eine Theorie der zellulären Automaten und wendete sie, ähnlich wie später Stephen Wolfram, auch auf die Kosmologie an.

Ein funktionstüchtiger Nachbau der Z3 steht heute im Deutschen Museum in München. Im Deutschen Technikmuseum Berlin befindet sich ein Nachbau der Z1. Dort steht auch eine komplette Z22 sowie eine bis vor kurzem noch funktionsfähige Z23V. An der Fachhochschule Karlsruhe war eine Z22 in kompletter Ausstattung bis 2005 funktionstüchtig in Betrieb (siehe Artikel c't 20/02, Seite 100). Anfang 2005 wurde sie im Rahmen einer Ausstellung im Zentrum für Kunst und Medientechnologie in Karlsruhe noch betriebsfähig aufgebaut und wird heute aufgrund des hohen Unterhaltungsaufwands (fast täglich defekte Röhren tauschen, die schon seit einem halben Jahrhundert nicht mehr serienmäßig produziert werden) nur noch selten betrieben. Über eine heute noch funktionsfähige Z25 aus dem Jahr 1967 verfügt das Arithmeum in Bonn.

1985 wurde Zuse das erste Ehrenmitglied der Gesellschaft für Informatik. Seit 1987 verleiht diese alle zwei Jahre die Konrad-Zuse-Medaille. Zuse ist seit 1995 Ehrenbürger der Stadt Hoyerswerda. Auf Initiative von Bill Gates traf sich Konrad Zuse mit diesem auf der CeBIT 1995. Ebenfalls 1995 wurde er für sein Lebenswerk mit dem Bundesverdienstkreuz ausgezeichnet. In diesem Jahr wurde er auch Ehrenmitglied im Chaos Computer Club. Er wurde 2003 im ZDF auf Platz 15 der größten Deutschen gewählt. Das Museum der Stadt Hünfeld hat ebenfalls eine Konrad-Zuse-Abteilung eingerichtet, die einige interessante Exponate (z. B. Z23, Z25, Z64 Graphomat) zeigt. Des Weiteren existiert in Hoyerswerda das Konrad-Zuse-Computermuseum, welches sich mit der Geschichte der Rechentechnik und dem Leben Zuses beschäftigt.

2002 wurde ein Konrad Zuse gewidmetes Medienzentrum an der Bauhaus-Universität Weimar eröffnet, das das Rechenzentrum der Hochschule sowie verschiedene Studios beherbergt. Elf Jahre zuvor hatte Zuse die Ehrendoktorwürde der Bauhaus-Universität erhalten.

Heute werden Ampelanlagen rechnergesteuert; Ihr Einkauf wird über Scannerkassen eingelesen; das Geld zum bezahlen erhalten Sie an Geldautomaten. Ihre Flugreise in den Süden wird im Reisebüro über den Computer gebucht; auf dem Flug dorthin hat der Pilot Zeit Ihnen über einen Monitor die Flugroute zu erklären, da der Autopilot gerade fliegt usw. Diese Beispiele aus unserem Alltag ließen sich beliebig fortsetzen.

3. Allgemeine Grundlagen

Lernziele:

Der/Die Lernende soll ohne Hilfsmittel und mit eigenen Worten:

- die Gründe und Ziele für den Einsatz von Informationstechnik erläutern können,
- die dabei entstehenden Probleme erkennen und benennen können,
- die Informationsarten beschreiben können,
- aufzählen können, welche einzelnen Verarbeitungsschritte und Auswertungsmöglichkeiten es in einem IT-System gibt,
- das Grundprinzip der elektronischen Datenverarbeitung verstehen und erklären können,
- Grundbegriffe richtig einordnen und verwenden können.

3.1. IT-Grundrecht

Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (umgangssprachlich auch als IT-Grundrecht, Computer-Grundrecht oder Grundrecht auf digitale Intimsphäre bezeichnet) ist ein in der Bundesrepublik Deutschland geltendes Grundrecht, welches vornehmlich dem Schutz von persönlichen Daten dient, die in informationstechnischen Systemen gespeichert oder verarbeitet werden.

Dieses Recht wird im Grundgesetz nicht eigens genannt sondern es wurde als spezielle Ausprägung des allgemeinen Persönlichkeitsrechts 2008 durch das Bundesverfassungsgericht derart formuliert bzw. aus vorhandenen Grundrechtsbestimmungen abgeleitet. Dieses Grundrecht wurde in den Leitsätzen des Urteils des Bundesverfassungsgerichts vom 27. Februar 2008 neu formuliert (Az. 1 BvR 370/07, 1 BvR 595/07).

Das Urteil erging aufgrund von Verfassungsbeschwerden gegen die Vorschriften im Verfassungsschutzgesetz von Nordrhein-Westfalen zur Online-Durchsuchung. Nach Maßgabe des Bundesverfassungsgerichts umfasst das allgemeine Persönlichkeitsrecht, welches sich aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 des Grundgesetzes ergibt, auch ein Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme.

Dieses Grundrecht ist subsidiär und tritt insbesondere gegenüber dem Telekommunikationsgeheimnis (Art. 10 Abs. 1 GG) und der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG) zurück. Es kommt also nur als „Auffanggrundrecht“ zur Anwendung, um Schutzlücken zu schließen.

3.2. Gründe für die Anwendung der Informationstechnik

Die Grundüberlegung beim Einsatz von Informationstechnik war es vor allem, sich bei der Erledigung von wiederkehrenden, eintönigen und zeitaufwendigen Tätigkeiten technischer Hilfsmittel zu bedienen.

Außerdem sollten einmal erhobene Informationen für die spätere erneute Benutzung aufgehoben werden können. Hinzu kam die Erkenntnis, dass nur durch den konsequenten Einsatz von Informationstechnik die ständig steigenden Datenmengen bewältigt werden können.

3.3. Entwicklung

Dienten früher Steintafeln und später Papier als Datenträger zur Aufzeichnung von Informationen, so wählen wir heute elektronische Verfahren. Der Meißel, die Schreibfeder und später die Schreibmaschine dienten zur mechanischen Aufbringung der Informationen auf das Trägermaterial.

Dieses wurde von der Rollenform zum standardisierten A4 Format weiterentwickelt. Für die Aufzeichnung von strukturierten Informationen wurden erst Tabellen verwendet, anschließend nutzte man Karteikarten. Diese, wie auch ihr Aufbewahrungsbehälter, der Karteikasten, sind wie andere mechanische Hilfsmittel seit Jahrzehnten in allen Büros vorhanden, verschwinden nun aber zunehmend.

Seit Anfang der 50er Jahre wurden diese Hilfsmittel durch Datenverarbeitungsanlagen (Computer) ergänzt und vielfach auch ersetzt. Durch ihren Einsatz können die ständig wachsenden Informationsmengen ohne eine gleichartig wachsende Personalausstattung bewältigt werden.

In der Datenverarbeitung werden entsprechende elektromagnetische Datenträger berührungsfrei, durch magnetisieren von „Eisenteilchen“ mit Informationen, „beschrieben“.

Bis weit in die 60er Jahre hinein wurde auch in der Datenverarbeitung noch mit mechanischen Datenträgern, den Lochkarten, gearbeitet. Erst die Entwicklung kostengünstiger elektromagnetischer Datenträger brachte hier den Durchbruch. Eine Festplatte mit einer Speicherkapazität von 5 Millionen Zeichen (ca. 4,77 Megabyte) kostete 1983 noch 15.000.-DM, heute kostet eine Festplatte mit einer Speicherkapazität von ca. 524 Millionen Zeichen (500 Megabyte) weniger als 100 Euro.

Der Vorteil der elektromagnetischen Datenträger ist die höhere Kapazität, die schnellere Suche und die leichte Handhabbarkeit. Die Datenverarbeitung (DV) wurde anfangs durch zentrale Rechenanlagen mit angeschlossenen Arbeitsplätzen, den Terminals, abgewickelt. Diese Arbeitsplätze bestehen aus einem Bildschirm, einer Tastatur

und einer Elektronik, die es ermöglicht, die am Terminal eingegebenen Daten zum Rechenzentrum zu übertragen und von dort die Verarbeitungsergebnisse wieder zu empfangen.

Die eigentliche Verarbeitung findet nicht im Terminal, sondern auf zentralen Rechenanlagen statt. Diese stehen in einem Rechenzentrum und werden dort von den Operatoren (wörtlich: Maschinenbediener) bedient. Sie stellen auf dieser zentralen Rechenanlage den Benutzern an den Terminals die zur Aufgabenerledigung benötigten Programme (Software) und Daten zur Verfügung, verwalten die Geräte (Hardware) und helfen bei der Behebung von Störungen.

Seit Anfang der 80er Jahre wird die bis dahin zentral vorgehaltene Rechnerleistung, nicht zuletzt bedingt durch die neuen Techniken der Mikrochips und der sich daraus ergebenden immer günstigeren Preis-/Leistungsrelation der Geräte, zunehmend dezentralisiert. Begriffe wie „Mittlere Datentechnik“, „Abteilungsrechner“ oder „Downsizing“ - sollen hier stellvertretend genannt werden, sie bezeichnen deutlich die Änderung der konzeptionellen Überlegungen bei der Abdeckung des DV-Bedarfs einer Firma oder einer Verwaltung; also weg von dem „zentralen Riesen“ hin zu einer verteilten, vor Ort verfügbaren Rechnerleistung.

Für den Endbenutzer wird die Dezentralisierung der DV besonders deutlich durch die in immer größerer Zahl eingesetzten PERSONAL COMPUTER (engl. personal = persönlich; also der Computer zur persönlichen Verwendung), den PC. Ein PC besteht gewöhnlich aus einem Monitor, einer Tastatur, einer Maus und einem ZENTRALGERÄT (CPU = Central Processing Unit, zentrale Verarbeitungseinheit). In diesem Zentralgerät findet die eigentliche Datenverarbeitung statt. Hier werden die Programme und die Daten gespeichert. Monitor, Tastatur und Maus sind an diesem Zentralgerät angeschlossen. Meist ist auch ein Arbeitsplatzdrucker angeschlossen.

Es gibt heute kaum einen Arbeitsplatz, an dem kein PC installiert ist oder der Einsatz eines PC zumindest konkret überlegt wird. PC sind völlig unabhängig von anderen DV-Systemen individuell einsetzbar. Sie können aber auch, wenn Daten ausgetauscht oder gemeinsam genutzt werden sollen, zu PC-Netzwerken verbunden werden. Ebenso ist es mittels spezieller Hard- und Software möglich, den PC als Client am zentralen Rechner zu betreiben.

Der PC bietet in den klassischen Anwendungsbereichen des Büroeinsatzes, also der **Textverarbeitung**, der **Tabellenkalkulation** und der **Datenverwaltung** gegenüber manuellen Verfahren erhebliche Vorteile:

- Wesentlich höhere Verarbeitungsgeschwindigkeit
- Höhere Zuverlässigkeit
- Effektivere Ablagetechniken

Der PC bietet ferner durch seine technischen Möglichkeiten und die immer leistungsfähiger und benutzerfreundlicher gestalteten Programme auch völlig neue Möglichkeiten der Aufgabenerledigung, z. B. „Electronic Mail“ (elektronische Post) oder das Benutzen von ex-

ternen Datenbanken über einen Anbieter von Fernverbindungen (z. B. CompuServe oder AOL) oder das Internet.

Insbesondere die Nutzung des Internets hat in den vergangenen Jahren um ein vielfaches zugelegt, da hier das Angebot umfangreicher geworden ist und die Nutzung auch für den ungeübten Anwender einfach ist.

In der Verwaltung wird der Begriff APC für Arbeitsplatzcomputer verwendet. Die Berliner Verwaltung hat seit den 90er Jahren die Nutzung von Computern in nahezu allen Bereichen forciert und abgeschlossen. Viele Fachanwendungen helfen den Dienstkräften bei der täglichen Arbeit. Die Entwicklung geht zügig voran.

3.4. Ziele des Einsatzes der Informationstechnik

Ziel des Einsatzes der Informationstechnik muss sein Informationen aktuell, schnell, im benötigten Umfang, wirtschaftlich, zum richtigen Zeitpunkt zur Verfügung zu haben und zu verarbeiten.

3.4.1. Aktuell

Ohne Zeitverzögerung stehen die aktuellen Daten allen Mitarbeitern zur Verfügung. So werden z. B. geänderte Adressdaten vom aufnehmenden Sachbearbeiter in einen zentralen Datenbestand eingegeben; sofort erhalten alle angeschlossenen Mitarbeiter bei einer Anfrage nach der betreffenden Adresse die neuen Daten.

3.4.2. Schnell

Der Zugriff auf die Informationen muss einfach und direkt möglich sein. Sie müssen permanent zur Abfrage zur Verfügung stehen. Bei der Sammlung der Informationen müssen bereits die späteren Abfragen berücksichtigt werden.

3.4.3. Im benötigten Umfang

Nicht alle Mitarbeiter benötigen zur Aufgabenerledigung alle Informationen. Jede Zielgruppe der Informationsverarbeiter benötigt die Informationen in einer anderen Stufe der Aufbereitung. Die zugänglichen Informationen müssen so zugeschnitten sein, dass die aktuelle Aufgabe erledigt werden kann. Zum Beispiel müssen dem Pförtner die Personaldaten so zur Verfügung gestellt werden, dass er auf die Informationen Namen, Abteilung, Stellenzeichen, Telefon-, Zimmernummer und Aufgabengebiet zugreifen kann. Andere Daten, wie z. B. Vergütungsgruppe sind nicht ablesbar.

3.4.4. Wirtschaftlich

Der Nutzen der Datenbereitstellung muss in einem vernünftigen Verhältnis zum dafür notwendigen Aufwand stehen. In einem Fall wollte eine Behörde mit einem jährlichen Aufwand von mehr als 170.000 €

alle zugänglichen Zeitungsausschnitte in einem datenbankgestützen Verfahren erfassen und verwalten.

Dies sollte den schnellen Zugriff auf einzelne Artikel, z. B. mit dem Suchbegriff „Wohnheim“ ermöglichen. Bei der Betrachtung der Wirtschaftlichkeit dieses Projektes ergab sich aber, dass eine solche Abfrage im Datenbestand höchstens zwei- bis dreimal jährlich zu erwarten war.

3.4.5. Verfügbarkeit zum richtigen Zeitpunkt

Die benötigten Informationen müssen für den Sachbearbeiter zu dem Zeitpunkt verfügbar sein, wenn er sie benötigt. Wenn der Antragsteller zur Sprechzeit erscheint, muss es sofort möglich sein, auf die erforderlichen Daten zuzugreifen. Außerdem muss es möglich sein, die weiteren Bearbeitungsschritte gleich einzuleiten.

3.5. Auswirkung auf das Verwaltungshandeln

In Zeiten knapper finanzieller Möglichkeiten muss auch die Verwaltung alle Maßnahmen zur Erhöhung der Wirtschaftlichkeit ergreifen. Eine Möglichkeit ist der Einsatz von Informationstechnik. Allerdings ist dieser Einsatz nur sinnvoll und wirtschaftlich, wenn begleitend zur Einführung der Informationstechnik auch Änderungen in der Aufbau- und Ablauforganisation und bei den diese Organisationsformen bestimmenden Vorschriften vorgenommen werden.

Eine bloße Übernahme bisher manuell ausgeführter Bearbeitungsschritte auf informationstechnisch unterstützte Abläufe ist meist unwirtschaftlich und nutzt in keiner Weise die besonderen Möglichkeiten der Informationstechnik.

3.6. Grenzen der Automatisierbarkeit in der Verwaltung

Die Verwaltung ist im Wandel. Sie ist auf dem Wege zu einer dienstleistungs- orientierten Organisation.

Viele Aufgabenstellungen der Verwaltung bedingt einen engen Kontakt zum Bürger, der eine personenbezogene Anlaufstelle benötigt, den Sachbearbeiter. Dieser lässt sich nicht automatisieren, d.h. durch einen Computer ersetzen.

Aber die von ihm angestoßenen und auszuführenden Arbeiten können, wie z. B. Wohngeldberechnung, Berechnung und Zahlbarmachung von Sozialhilfe oder Erziehungsgeld, von der Informationstechnik erledigt werden.

Dadurch wird die Aufgabenerledigung der Verwaltung beschleunigt und somit kostengünstiger. Die Unterstützung durch die Informationstechnik findet aber auch Ihre Grenzen. So lässt sich der Pfört-

nerdienst, vergleichbar mit der Fahrplanauskunft, nicht auf Computer umstellen.

Die Vielzahl der möglichen Aspekte der auftretenden Fragen und die zu erwartenden Schwierigkeiten der Bürger mit so einem computergesteuerten Auskunftsdienst lassen einen derartigen Einsatz der Informationstechnik nicht zu. Es ist aber unverständlich, warum viele Pförtner und auch Telefonzentralen noch immer in meist veralteten Listen wühlen, wenn man einen Sachbearbeiter oder dessen Telefonnummer erfragt. Hier ist mit wenig Aufwand eine wesentliche Verbesserung zu erreichen, denn die Daten sind ja in den Computersystemen der Verwaltung vorhanden.

Bei der Zuteilung von PC wird oftmals sehr restriktiv verfahren. Dies führt dazu, dass sich mehrere Mitarbeiter einen Computer - Arbeitsplatz teilen müssen. Leider spiegelt sich das auch immer wieder bereits bei der Ausbildung am PC schon in der Verwaltungsakademie wieder, da sich aus den unterschiedlichsten Gründen mehrere Lehrgangsteilnehmer einen Schulungs-PC teilen müssen.

Eine optimale, aufgabenorientierte Einbindung der Informationstechnik in den Arbeitsablauf wird so unmöglich gemacht. Hinzu kommt, dass die Ausbildung der Mitarbeiter oft nicht rechtzeitig oder umfassend genug erfolgt. Auch werden Programme eingesetzt, die den international üblichen Mindestanforderungen nicht entsprechen. So war beim Haushaltswesenprogramm PROFISKAL der Eingabestandort durch das Fehlen der Cursoranzeige nicht zu ermitteln.

Das Berliner Datenschutzgesetz regelt den Umgang der Verwaltung mit personenbezogenen Daten. Auf Grundlage dieses Gesetzes und des Bundesdatenschutzgesetzes ergibt sich regelmäßig eine unterschiedliche Beurteilung dessen, was technisch möglich, politisch wünschenswert und aus Datenschutzgesichtspunkten durchführbar ist. Ein Beispiel ist die Frage der Zulässigkeit der Vernetzung der Sozialämter und die Weitergabe der Daten von Asylbewerbern.

Oft sind es aber organisatorische Defizite, die auf die modernen Verhältnisse in der Verwaltung angepasst werden müssen. Das folgende Beispiel soll einen anderen Aspekt der Problematik des effektiven Einsatzes von Informationstechnik in der Verwaltung verdeutlichen:

Ein Mitarbeiter war sehr bemüht sein Textverarbeitungsprogramm so einzurichten, dass dieses genau in die für die Einfügungen vorgesehenen Freiräume auf dem im Drucker eingespannten Vordruck schreibt. Die Möglichkeit, den ganzen Vordruck in das Textsystem aufzunehmen und dann Standardtext und Einfügungen zusammen aus dem Textsystem auszudrucken - was die für die Textverarbeitung übliche Vorgehensweise ist - wurde durch die Vorschrift, dass dieser Vordruck so benutzt werden muss wie er ist, unmöglich gemacht.

Vorschriften verhindern auch den Einsatz kostenloser Hilfemöglichkeiten. Manche Programmhersteller bieten eine kostenfreie „Hotline“ (telefonische Hilfestellung) an, die über eine „0130“ bzw. „0800“ Telefonnummer zum Ortstarif angewählt werden kann.

Leider ist aber oftmals der „normale“ Mitarbeiter der Verwaltung nicht berechtigt „Ferngespräche“ zu führen.

3.7. Die Informationstechnik

Die Datenverarbeitung - eigentlich der streng technisch gefasste Begriff für die zur Verarbeitung der Daten eingesetzten Technik - wurde zusammen mit den zur Verarbeitung der Informationen eingesetzten Programme zum Begriff Informationstechnik zusammengefasst.

Der so entstandene Begriff der Informationstechnik umfasst somit die Bereiche der klassischen Datenverarbeitung (DV), also Großrechenanlagen und mittlere Datentechnik bis hin zu modernsten Parallelrechnern, ebenso die PC und die allgemeine Bürotechnik.

Außerdem gehören streng genommen auch noch die manuelle DV (Karteikarten und Karteikasten), die mechanische DV (Abakus, Rechenschieber und die manchmal noch anzutreffende mechanische Rechenmaschine) sowie die elektromechanische DV (Lochkarte, Lochstreifen) dazu.

Informationstechnik

umfasst Geräte und Verfahren zur automatisierten Erfassung, Darstellung, Speicherung und Verarbeitung von Informationen.

Zum besseren Verständnis sollen hier noch einmal die beiden Begriffe „Information“ und „Kommunikation“ näher betrachtet werden.

Information

Unter Information versteht man in der Umgangssprache die Kenntnis über Sachverhalte und Vorgänge (Hansen Wirtschaftsinformatik 5. Auflage, S. 63).

Jeder Austausch von Informationen zwischen mindestens zwei Beteiligten stellt eine Kommunikation dar. Dabei wird davon ausgegangen, dass die an der Kommunikation Beteiligten eine gemeinsame 'Sprache' sprechen.

Die Kommunikation kann in zwei grundsätzlich unterschiedlichen Formen erfolgen. Zu unterscheiden sind:

- Der Austausch nur in Richtung Sender → Empfänger, es erfolgt eine unidirektionale1 Kommunikation. Der Empfänger kann die bei ihm eintreffenden Informationen sammeln bis er den Befehl zur Verarbeitung erhält. Diese Arbeitsweise ist möglich, weil die nächste Datenübermittlung durch den Sender nicht von der Wahrnehmung und Berücksichtigung des Ergebnisses der vorhergehenden Verarbeitung abhängig ist. Diese Arbeitsweise des Ansammelns von Daten zur Verarbeitung, und die Verarbeitung aller gesammelter Daten erst auf einen besonderen Befehl

hin, nennt man Batch - Betrieb, also einen Stapel von Informationen verarbeiten.
- Der Austausch der Informationen in Richtung Sender → Empfänger und nach sofortiger Verarbeitung der empfangenen Information eine Übermittlung des Verarbeitungsergebnisses in Richtung Empfänger → Sender.

Wenn eine solche bidirektionale2 Kommunikation vorhanden ist, spricht man vom Dialog. Dies ist die heute übliche Arbeitsweise beim Einsatz von PC.

Kommunikation

ist der Austausch von Informationen zwischen einem Sender und mindestens einem Empfänger. Dabei wird davon ausgegangen, dass beide Seiten eine „Sprache“ verwenden.

Kommunikation als Begriff der Informations- und Kommunikationstechnik (IuK) beinhaltet die Bereiche Netzwerke, Bürokommunikation und weltweiter Datenaustausch.

Daten

Aus Zeichen zum Zweck der Verarbeitung gebildete Informationen heißen Daten. (Hansen Wirtschaftinformatik S. 7)

3.8. Informationsarten

Unter Berücksichtigung der Betrachtungstiefe an dieser Stelle ist es ausreichend, Informationen mit Daten gleichzusetzen.

Um die verschiedenen Möglichkeiten der Informationsverarbeitung beurteilen zu können, ist es wichtig zu wissen, wie Informationen, hier insbesondere im Bürobereich, auftreten können. Aus diesen verschiedenen Erscheinungsformen ergeben sich auch äußerst unterschiedliche Anforderungen an die bei ihrer Verarbeitung einzusetzende Technik.

Betrachtet man eine Textseite, z. B. einen Brief, so lässt sich dieser in Absätze, diese in Sätze, diese in Worte und diese in einzelne Zeichen auflösen. Das einzelne Zeichen ist also in den verschiedensten Zusammensetzungen die Informationsform, die wir am Häufigsten antreffen.

3.8.1. Texte und Zahlen

Texte sind Informationen die aus Buchstaben, Ziffern und Sonderzeichen zusammengesetzt sind. Dazu gehören die

3.8.1.1. Alphazeichen (A – Z und a – z)

Für den Computer kommen also in der Reihenfolge der Berücksichtigung zuerst die Großbuchstaben, dann erst mit einigem Abstand die

Kleinbuchstaben. Dies macht sich manchmal beim Sortieren unschön bemerkbar. So sollte bei alphabetischer Sortierung einer Namensliste „von Schulze' nicht nach „Zappe' einsortiert werden.

3.8.1.2. Numerische Zeichen (∅ – 9)

Die numerischen Zeichen beginnen mit der Null (in der Informationstechnik mit einem Schrägstrich geschrieben ⌀, damit sie deutlich vom großen „O" zu unterscheiden ist, aufsteigend bis zur 9, insgesamt also 10 Ziffern, da bei uns das Dezimalsystem gilt.

3.8.1.3. Sonderzeichen

Allgemeine	**. ; : ! ?**
Länderspezifische	ö ä ü ß §
Steuerzeichen	z. B. Zeilenschaltung:
	Tabulator, Leertaste

Sonderzeichen ergänzen die Buchstaben und Ziffern. In der Informationstechnik können sich Sonderzeichen als sehr tückisch erweisen und konnten/können nicht uneingeschränkt verarbeitet werden. Besonders bei Briefen oder Adressaufklebern die mit Hilfe von Großrechnern erstellt worden sind, heißt Familie Müller oft schlicht Mueller, im Extremfall noch in Großbuchstaben.

Die tückischen Eigenschaften von Sonderzeichen führten auch dazu, dass ein für die juristische Fakultät einer norddeutschen Universität auf Empfehlung einer Expertenkommission beschaffter Großrechner nicht wie geplant eingesetzt werden konnte - der Rechner konnte das §-Zeichen nicht verarbeiten.

In Publikationen und Handbüchern findet sich gelegentlich der Begriff „alphanumerischer Zeichensatz". Gemeint ist damit die Gesamtheit der darstellbaren Zeichen, nämlich Alphazeichen, numerische Zeichen und die Sonderzeichen, insgesamt 128 Zeichen (ASCII3), bzw. 256 Zeichen (EBCDIC4), wobei nicht alle Zeichen darstellbar sind.

Texte werden zunehmend durch graphische Elemente ergänzt. Diese können die klassischen Grafikelemente wie Linien, Kreis etc. beinhalten aber auch Fotos, Bilder oder Pictogramme, sogenannte Logogramme, abgekürzt Logos.

3.8.2. Logogramme/Pictogramme

Diese symbolhaften Darstellungen sind ohne Worte international verständlich. Sie wurden zum ersten Mal bei den olympischen Spielen 1972 in München eingesetzt, bei denen jede Sportart „ihr Logo" erhielt. Pictogramme sind die wesentlichen Elemente der nonverbalen Kommunikation.

Sie werden z. B. zur sprachlosen Mitteilung von Verboten und Hinweisen eingesetzt. Sie verwenden symbolhafte Darstellungen, z. B. für Notausgang, Nichtraucher, Damen- oder Herrentoilette. Dieser Bereich der nonverbalen Kommunikation gewinnt wegen der sprachübergreifenden Verständigungsmöglichkeiten zunehmend an Bedeutung.

3.8.3. Grafik

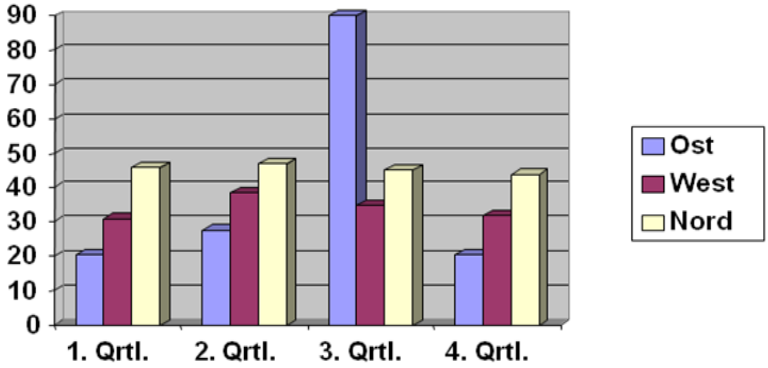
frei gestaltete Grafik:

Dazu zählt jedes Zeichnen am Computer, aber auch der Entwurf von Landkarten und technischen oder Bauzeichnungen. Man spricht hier von CAD (Computer aided Design, computerunterstütztes Entwerfen).

Dafür wird ein schneller und leistungsfähiger Rechner, ein entsprechendes Programm und bei größeren Ausgabeformaten ein spezielles Zeichengerät, der Plotter benötigt.

Geschäftsgrafik (engl. Businessgraphics):

Darunter versteht man die Arten Linien-, Balken- und Kreisdiagramme; diese Darstellungen sind beispielsweise von jedem Wahlabend bekannt.



3.8.4. Foto/Video

Bilder beinhalten mehrere Informationsebenen, d.h. jeder Betrachter sieht ein Bild mit anderen Augen, achtet auf andere Einzelheiten. Vielleicht kennen Sie auch den schönen Test „Wären Sie ein guter Augenzeuge?“ - fünf Minuten wird ein Bild betrachtet, dann müssen Fragen dazu beantwortet werden. Bei den Antworten kann man manchmal nicht glauben, dass alle Befragten gerade dasselbe Bild gesehen haben. Deshalb wird versucht, die Aussage eines Bildes eindeutig zu machen, z. B. durch Entfernen des Bildhintergrundes; der Betrachter soll sich nur auf den Vordergrund konzentrieren und nicht abgelenkt werden. Dies kann gut an Politikerfotos in den Nachrichtensendungen beobachtet werden.

Fotos können heute so perfekt manipuliert werden, dass die Veränderungen nicht zu bemerken sind. Früher passierte es schon mal, dass dabei noch ein Arm oder ein Fuß auf dem Foto verblieb. Heute gelingt selbst der Schattenwurf. Auch bewegte Bilder werden perfekt gestaltet. Es müssen ja nicht immer die Dinos im „Jurassic Park“ sein. Seit die Bildbearbeitungsprogramme - auch für den Heimbereich - so

verbessert worden sind, gibt es eigentlich keine Fotos etc. mehr, die eine absolute Beweiskraft haben.

Beim Verarbeiten von Fotos/Videos entstehen sehr viele Daten, die in jeder Phase der Verarbeitung angefasst werden müssen. Daraus ergibt sich, dass nur leistungsfähige schnelle Systeme mit großem Speicher zur Verarbeitung verwendet werden können. Eine DIN A4 Seite als Zeichenfolge dargestellt ergibt einen theoretischen Speicherbedarf von ca. 3300 Zeichen, in der Praxis meist nur 2000 bis 2500 Zeichen. Dieselbe Seite als Bild, also als eine Folge von hell/dunkel Informationen verarbeitet, bedeutet theoretisch eine zu verarbeitende Datenmenge von 1,5 Millionen bei entsprechender Auflösung von 8 Millionen Zeichen.

3.8.5. Sprache

Die häufigste Form der Kommunikation ist das gesprochene Wort. Erst durch die Entwicklung leistungsfähiger Systeme ist es möglich geworden, die Sprache in allen Verwendungsvarianten in der Informationstechnik zu verarbeiten.

Wir unterscheiden folgende Verarbeitungsstufen:

- **Spracheingabe, Spracherkennung**
  Rein technisch bereitet es keine Schwierigkeiten, die analoge Schallschwingung der Sprache in eine für den Computer verarbeitbare digitale Darstellung umzuwandeln. Bei der Tonaufzeichnung auf CD ist dies an der Tagesordnung. Das Problem für die Spracherkennung war die Individualität des Sprechenden, die Eigenheiten der Aussprache und anfangs sogar der Unterschied, ob man erkältet war, heiser war oder „normal“ sprach. So war es lange Zeit notwendig jedes Wort, das der Computer erkennen sollte, mit diesem zu „üben“. Erst die jetzt verfügbaren leistungsfähigen Komponenten können, manchmal erst nach einer kurzen „Übungsphase“ in der ein Standardtext gesprochen wird, jedes beliebige Wort erkennen.

- **Sprachverarbeitung**
  Durch die moderne Spracherkennung ist es möglich, dem Computer zu „diktieren“, d.h. der Benutzer spricht in ein Mikrofon und der gesprochene Text erscheint auf dem Bildschirm, als sei er über die Tastatur eingegeben worden - selbstverständlich hinsichtlich Rechtschreibung und Zeichensetzung einwandfrei. Ein Teil dieses Lehrbriefes ist so entstanden. Anwendungen der Spracherkennung und -verarbeitung sind auch die Steuerung von Behindertenautos, die Paketverteilung, die Steuerung von Abläufen allgemein und die Zugangskontrolle.

- **Sprachausgabe**
  An die Zeitansage, die Fernsprech- oder Fahrplanauskunft oder die Ansagen auf den Flughäfen denkt man hier sicherlich sofort; es ist aber auch durchaus möglich, ein auf dem Computer geschriebenes Textdokument mit einer gesprochenen Anmerkung oder einem Korrekturhinweis zu ergänzen, der, vom Leser angestoßen, über einen Lautsprecher ausgegeben wird.

- **Sprachspeicherung**
  Digitalisierte Schallinformationen können auf jedem Datenträger gespeichert werden. Viele moderne Nebenstellentelefonanlagen lassen dies zu. Auch die „Anrufbeantworter“ der Mobiltelefone sind nur Computer, in denen die Informationen auf einer Festplatte digital gespeichert werden.

3.8.6. Signale, Messwerte

Die analogen Messwerte werden durch Sensoren aufgenommen und wie die Töne durch einen Analog/Digital-Wandler in digitale Informationen umgewandelt. Diese Ist-Werte werden dann im Computer mit den Soll-Werten verglichen. Bei Abweichungen werden entsprechende Steuerimpulse ausgelöst. Dies ist die klassische Form des eigentlich aus der Biologie bekannten Regelkreises. Als Beispiele seien hier die Klimaanlage, die dynamische Ampelsteuerung sowie die Verkehrsbeeinflussungsanlagen genannt.

3.9. Digitale und analoge Daten

Bei analogen Daten (analog = vergleichbar) handelt es sich um Daten, die durch eine Skala (z. B. Thermometer), durch eine Zeigerstellung (Uhr) oder ähnliches dargestellt werden.

Digitale Daten (digit = Zahl) werden immer durch Ziffern dargestellt (Digitaluhr).

Rechnerinterne Verarbeitung

Alle Daten die der Computer verarbeitet, werden digital verarbeitet. Das heißt, alle Datentypen die der Computer empfängt, werden zuerst in digitale Daten umgewandelt und können so verschlüsselt weiterverarbeitet werden.

Die elektrische Art der Datenübermittlung basierte schon immer auf der Übermittlung durch codierte Informationen. Beim Morsen wurden Buchstaben in einen Morsecode übersetzt und übertragen. Mit den Darstellungsmöglichkeiten „kurzer Stromimpuls“, „langer Stromimpuls“ ein Standard vereinbart, der der Codierung dienen sollte.

Das Morsealphabet z. B. SOS = ... --- ...

Der Computer versteht auch nicht viel mehr, denn er arbeitet ebenfalls nur mit Stromimpulsen. Die kleinste Informationseinheit eines Computers ist ein Schalter:

Binäres System

- Schalter können an (Strom fließt) oder aus (Strom fließt nicht) sein. Ein Schalter kann somit zwei Zustände annehmen.
- Verschiedene Schalterstellungen bewirken verschiedene Aktionen des Rechners (analog: Toaster, wenn an toastet er, wenn nicht

dann eben nicht. Ein Computer ist jedoch vielseitiger, somit gibt es mehrere Schalter für verschiedene Aktionen).

- Ein solcher Schalter (die kleinste interne Organisationseinheit eines Computers) wird im EDV-Sprachgebrauch auch ein BIT (engl.: binary digit, deutsch: Binärzeichen) genannt. Dies liegt daran, dass ein System welches nur zwei Zustände darstellen kann binäres System genannt wird. Andere binäre Systeme sind z. B. das Dualsystem, das Morsealphabet, die Lichtzeichenanlage (Ampel), ...

Dualsystem

Um das Binärsystem des Computers dem Menschen verständlich zu machen, verwendet man keine Schaltpläne sondern das Dualsystem (binäres Zahlensystem bestehend aus den Ziffern 0 und 1).

Wäre der Rechner intern „BITweise“ organisiert, wäre dies sehr unpraktisch, da mit einem BIT wie gesagt nur zwei Zustände darstellbar sind, in aller Regel jedoch mehr Zustände benötigt werden.

Aus diesem Grund werden in einem Computer zur rechnerinternen Verarbeitung 8 BITs konstruktionstechnisch zu einem Byte zusammengefasst.

Das Wort Byte ist künstlich und stammt vom englischen bit (deutsch: Bisschen) und bite (deutsch: Biss). Verwendet wurde es, um eine Speichermenge oder Datenmenge zu kennzeichnen, die ausreicht um ein Zeichen darzustellen.

Der Begriff wurde 1956 von Werner Buchholz geprägt in einer frühen Designphase eines IBM-Computers. Im Original beschrieb er eine Breite von 6 Bit und stellte die kleinste direkt adressierbare Speichereinheit eines Computers dar. Die Schreibweise Bite wurde zu Byte geändert, um versehentliche Verwechslungen mit Bit zu vermeiden.

Byte wird als Abkürzung gedeutet für:

- Binary tuple
- Binary term
- Bit asynchronous transmission entity
- Binary yoked transfer element
- Binary digits unite
- Kombination aus den Worten „Bit“ und „Eight“

Eine weitere Erklärung des Begriffes liegt in der Kurzform „by eight“, übersetzt „mal acht“.

So ist der Zentralspeicher, der intern aus verschiedenen Speicherzellen besteht, byteweise organisiert, d.h. eine Speicherzelle kann genau ein Byte aufnehmen.

Auch der Prozessor und die Datenbusse sind byteweise organisiert. Mit dieser Organisationseinheit können 256 (28) Zustände dargestellt werden, also die Zahlen: 0, 1, 10, 11, 100, 101, 110, 111, ...

Mit einem Byte können somit sowohl die Befehle, als auch die Daten codiert werden:

Die Verwendung eines Systems, das nur zwei Zahlen verwendet, hat erhebliche Vorteile. Alle Daten lassen sich auf verschiedene Arten darstellen, weitergeben und verarbeiten. Diese Zahlen sind 0 und 1.

Nutzungsart	Ziffer 0 =	Ziffer 1 =
Transport innerhalb des Computers	Stromimpuls	kein Stromimpuls
Optische Speicherung	Medium undurchsichtig (kein Loch)	Medium durchsichtig (Loch)
Übertragung mit Tönen	kurzer Ton	langer Ton
Speicherung mit Magnetismus	magnetisches Feld vorhanden	Kein magnetisches Feld vorhanden

Theoretisch ist es auch möglich, anstelle der zwei Zustände mit den zehn Zuständen des Dezimalsystems zu arbeiten. Der technische Aufwand hierfür wäre immens. Oben sehen Sie, dass bei verschiedenen technischen Nutzungsarten das Dualsystem relativ problemlos funktioniert.

Wie lassen sich nun Texte und Zahlen vom Computer auf Grundlage des Dualsystems verarbeiten?

- Im Dezimalsystem (Zehnersystem) hat jede Stelle einer Zahl einen Stellenwert. Die Zahl 4711 beinhaltet Einer-, Zehner-, Hunderter- und Tausenderstellen.

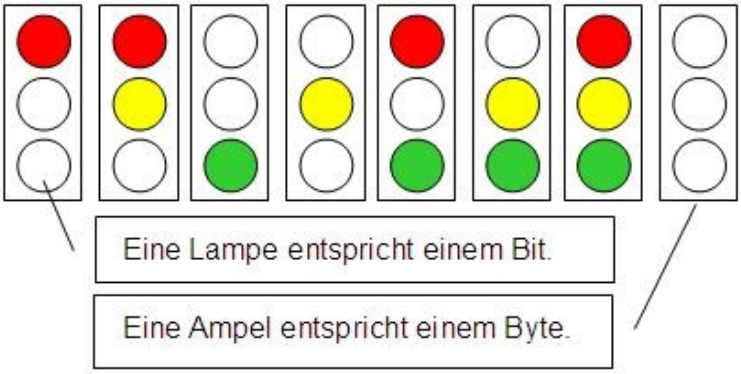
- Im Dualsystem hat auch jede Stelle einer Zahl einen Stellenwert.

Man spricht von Einern, Zweiern, Vierern, Achtern, Sechzehnern usw. Anhand dieser Kombinationen lassen sich ebenfalls alle Zahlen darstellen. Die Zahl 3 sieht dann nur so aus: 00000011

1.	2.	3.	4.	5.	6.	7.	8.
128	64	32	16	8	4	2	1
0	0	0	0	0	0	1	1
							3

Sie sehen, dass sich alle Zahlen auch mit dieser Schreibweise darstellen lassen, es erfordert nur etwas Kopfarbeit; nach dem Motto: „Welche Zahl der oberen Zahlenreihe passt in die gewünschte Zahl, füge an dieser Stelle eine 1 hinzu, nimm den Rest und verfahre genauso bis kein Rest übrigbleibt."

Für Texte ist es sehr ähnlich. Allerdings liegt dem Computer eine Liste vor, in der einer achtstelligen dualen Zahl ein ganz bestimmtes Zeichen zugeordnet wird. Dies ist die sogenannte ASCII-Tabelle.
Die Darstellung eines Zeichens mit dem Zustand 0 oder 1 nennt man Bit.
Insgesamt 8 Bit ergeben die Darstellung eines Zeichens. Dieses wird wiederum als Byte bezeichnet.



Die Einheit Byte ist die Maßeinheit für Speicherkapazitäten. Bei allen Computerspeichern kennzeichnet die Kapazität in Byte, wie viel Zeichen der Speicher gleichzeitig aufnehmen kann.

Folgende Speichergrößen werden verwendet, sind aber teilweise (noch) nicht gebräuchlich, da der technische Fortschritt derzeit noch Grenzen hat:

Name (Symbol)	**SI[1]-konforme Bedeutung**	**entspricht**
Kilobyte (KB)	10^3 Byte = 1.000 Byte	1024 B
Megabyte (MB)	10^6 Byte = 1.000.000 Byte	1024 kB
Gigabyte (GB)	10^9 Byte = 1.000.000.000 Byte	1024 MB
Terabyte (TB)	10^{12} Byte = 1.000.000.000.000 Byte	1024 GB
Petabyte (PB)	10^{15} Byte = 1.000.000.000.000.000 Byte	1024 TB
Exabyte (EB)	10^{18} Byte = 1.000.000.000.000.000.000 Byte	1024 PB
Zettabyte (ZB)	10^{21} Byte = 1.000.000.000.000.000.000.000 Byte	1024 EB
Yottabyte (YB)	10^{24} Byte = 1.000.000.000.000.000.000.000.000 Byte	1024 ZB

3.10. Erfassen, Verarbeiten und Ausgeben von Informationen

Informationsverarbeitung

Um eine Information in einem System der Informationstechnik verarbeiten zu können, muss diese Information dem System bekannt sein; d.h., die Information ist entweder gerade erfasst worden oder steht von einer früheren Eingabe her durch Speicherung und erneutem Aufruf zur Verfügung.

[1] Internationales Einheitensystem (SI)

Eine Information wird in vier Einzelschritten verarbeitet, von denen aber nicht immer alle Schritte durchlaufen werden müssen.

E	**ingabe**	
V	erarbeitung	
A	usgabe und	
S	peicherung,	(wenn die Information für eine spätere erneute Nutzung aufgehoben werden soll)

Diese Einzelschritte ergeben das so genannte EVA-Prinzip, hier ergänzt durch das Speichern, also ganz genau genommen das EVAS-Prinzip.

Diese Aufteilung in die grundsätzlichen Verarbeitungsschritte gilt für alle informationsverarbeitenden Systeme, auch für die bisherigen manuellen Verfahren.

Betrachten wir nun die einzelnen Verarbeitungsschritte in einem System der Informationstechnik:

Hier werden Informationen verarbeitet durch

- **Eingeben**
  über Tastatur, Spracheingabe, Datenübertragung, Seitenleser etc. (s. nachfolgend „Eingabegeräte“).

- **Speichern / Sichern**
  die meist auf dem Bildschirm sichtbaren Informationen werden für eine spätere erneute Nutzung abgelegt; vergleichbar dem Ablegen von Informationen, die auf dem Schreibtisch sind in einer Registratur.

- **Laden / Öffnen**
  entspricht dem Suchen und Finden von Informationen in einer Registratur und dem anschließenden Transport dieser Informationen auf den Schreibtisch.

- **Ausgeben**
  jede Darstellung von eingegebenen, gespeicherten oder als Verarbeitungsergebnis gewonnenen Informationen zur optischen, akustischen oder sonstigen Wahrnehmung ist eine Ausgabeoperation; die gängigen Ausgabegeräte sind Bildschirm und Drucker.

- **Bearbeiten / Ändern**
  zu unterscheiden sind inhaltliche Änderungen, das Editieren und das Verändern des äußeren Erscheinungsbildes, das Layout der Information, dem Formatieren.

- **Löschen**
  ist das Entfernen einer oder mehrerer Informationen aus einer Folge von Informationen (Informationssammlung, Datei) oder das

Entfernen einer Informationssammlung aus einem Speicher oder von einem Datenträger. Nicht jede Information, die nicht mehr sichtbar, bzw. nicht jede Datei, die nicht mehr im Inhaltsverzeichnis aufgeführt wird, ist wirklich, d.h. physikalisch entfernt. Mit entsprechenden Programmen können gelöschte Daten wieder zugänglich gemacht werden. Hier kann es erhebliche Probleme hinsichtlich des Datenschutzes geben.

- **Mathematische Operationen**
  Verknüpfung von numerischen Informationen mittels der auf die Grundrechenarten zurückgeführten Verarbeitungsregeln (Addition, Subtraktion, Multiplikation, Division).

- **Zählen**
  Obwohl vielfach vermutet, keine mathematische Operation. Das Zählen, also das Erhöhen eines Speicherinhalts in definierten, gleichbleibenden Schritten, wird in DV-Anlagen einfacher und damit schneller abgewickelt als durch eine Addition.

- **Logische Operationen**
  Die zu verarbeitenden Informationen werden entsprechend ihrer Bedeutung in Beziehung zueinander gesetzt. Mögliche Kombinationen sind: und, oder, wahr, unwahr.

Die letzten drei Verarbeitungsmöglichkeiten werden auch unter dem Sammelbegriff „Auswerten“ zusammengefasst.

- **Auswertungsmöglichkeiten**

  - **Mischen**
    Informationen werden mittels eines Zufallsgenerators in eine neue Reihenfolge gebracht.
  - **Sortieren**
    Informationen werden entsprechend ihres Inhalts in eine geordnete Reihenfolge gebracht; aufsteigend oder absteigend entsprechend dem angegebenen Sortierkriterium.
  - **Kombinieren**
    Aus mehreren getrennten Datenbeständen wird ein neuer gemeinsamer Datenbestand erzeugt.
  - **Verknüpfen**
    Mehrere getrennte Datenbestände werden über eine in allen diesen Datenbeständen vorhandene gleiche Information in eine Beziehung zueinander gesetzt (Relation); die Datenbestände bleiben aber getrennt, die Beziehung kann jederzeit wieder aufgelöst werden.
  - **Selektieren**
    Aus einem Datenbestand werden alle Informationen herausgesucht, die einem angegebenen Kriterium entsprechen.
  - **Entscheiden**
    Informationen entsprechend einem vorgegebenen Auswertungsmuster (Programm) verarbeiten und aus dem Verarbeitungsergebnis resultierende Folgeaktionen ausführen.

Immer wieder liest man, dass Computer „entscheiden“. Das Entscheiden setzt aber Kreativität voraus. Ein Computer kann jedoch nur in den Grenzen reagieren, die ihm in Form von Programmen vorgegeben sind. Im diesem Zusammenhang werden immer wieder zwei Begriffe benutzt:

- Künstliche Intelligenz, KI (engl. artificial Intelligence, abgk. AI.)
  Ist der Versuch, einem Computer ein menschenähnliches Handeln auf der Grundlage von Wissen, Erfahrungen und Schlussfolgerungen beizubringen. Diese Thematik wird seit ca. 40 Jahren verfolgt. Das Ziel einen Computer in die Lage zu versetzen, jede menschliche Tätigkeit für die wir das, was wir Intelligenz nennen, voraussetzen, zu erledigen ist wahrscheinlich in absehbarer Zeit nicht zu erreichen. Das Problem sind vor allem die äußerst komplexen Verarbeitungsregeln (Algorithmen).

- Expertensystem („wissensbasiertes System“)
  Aktionen und Folgerungen, die auf der Auswertung von Informationen beruhen, werden vom Rechner ausgeführt. Basis ist dabei ein Schema, dass vor der Erstellung des Programms auf der Grundlage der menschlichen Handlungsweise angefertigt wurde.

Beispiel: Das Programm „Wie herzinfarktgefährdet sind Sie?“ beruht auf einem Fragebogen, der im Dialog Patient/Arzt ausgefüllt wurde. Der Arzt hat dabei die Antworten des Patienten bewertet und entsprechend die nächste sinnvolle Frage gestellt.

Auf der Grundlage der gesammelten Bewertungen der Einzelantworten wurde eine abschließende Auswertung erstellt. Dieser Ablauf des Patient/Arzt-Dialoges ist in allen seinen Verzweigungsmöglichkeiten erfasst und in ein Programm umgewandelt worden.

http://www.infarkt-test.de/webseite.html

Weitere Beispiele gibt es in der Versicherungswirtschaft - „Sind Sie richtig versichert?“ (Versicherungsrechner gibt es bei jeder großen Versicherung) und in anderen Bereichen, wo häufig gleiche Interaktionen ablaufen und bewertet werden müssen.

Fragen zur Selbstkontrolle:

1. Welche Vorteile bietet der Einsatz von PC gegenüber manuellen Verfahren?
2. Nennen Sie Ziele des Einsatzes der IT!
3. Welche Probleme existieren bei der Automatisierung der Verwaltung?
4. Was ist unter Informationstechnik zu verstehen?
5. Welche Formen der Information gibt es?
6. Welches Zahlensystem liegt der elektronischen Datenverarbeitung zugrunde?
7. Was bedeutet die Bezeichnung Bit?
8. In welchen Maß- oder Größenangaben werden Speicherkapazitäten in der IT angegeben? Nennen Sie dazu zwei Werte!
9. Wie lautet das Grundprinzip der Datenverarbeitung?

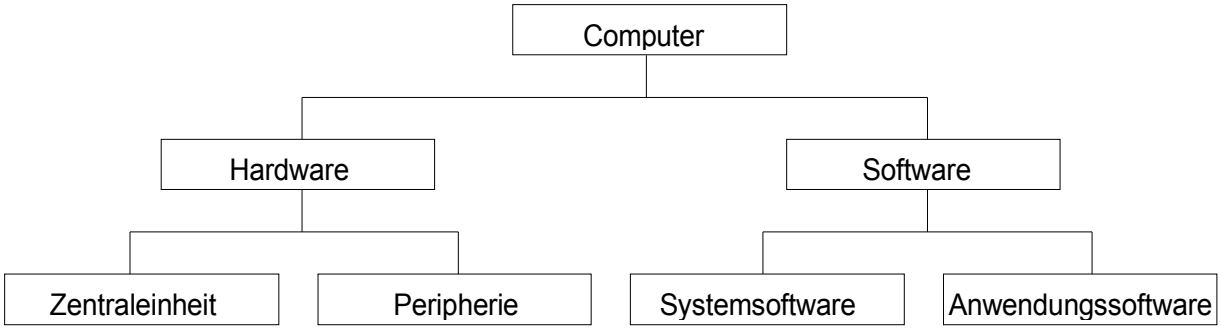
4. Aufbau der Informationstechnik

Lernziele:

Der/Die Lernende soll:

- den Unterschied zwischen Hardware und Software erklären können,
- wissen, welche Bauteile als Hardware bezeichnet werden,
- die grundlegenden Bestandteilen ein Computer nennen können,
- Eingabe- und Ausgabegeräte nennen können,
- die externen physikalischen Speichermedien nennen können,
- erklären können, warum für den Betrieb eines Computers ein Betriebssystem notwendig ist,
- welche Hauptaufgaben ein Betriebssystem zu erledigen hat,
- welche bekannten Betriebssysteme es gibt,
- was Dateien sind,
- welche wichtigen Programmarten existieren und für welche Anwendungsgebiete diese gedacht sind,
- welche typische Fähigkeiten und Merkmale die in der Verwaltung eingesetzten Programmen besitzen.

Zuerst einen Überblick der Bestandteile eines Computers



4.1. Hardware

Sämtliche Geräte und elektronischen Bauteile (alles was man in „die Hand nehmen kann") werden als Hardware bezeichnet (engl. Eisenwaren).

Dies sind bei einem Computer z. B. das Rechnergehäuse, die Speicherchips, die Tastatur etc. Die Diskette ist ebenso zur Hardware zu rechnen, nicht jedoch die darauf befindlichen Programme. Die Hardware ist also im Bereich der Computer unmittelbar an die Software gekoppelt.

4.1.1. Eingabegeräte

4.1.1.1. Die Tastatur

Obwohl die Tastatur neben dem Bildschirm unmittelbar vom Benutzer benötigt und häufig benutzt wird, führt sie doch z. B. in Bezug auf die Bedeutung der Speichermöglichkeit eines Rechners eher ein Schattendasein.

Während das äußere Aussehen eines Rechnergehäuses eher sekundär ist, fällt dieses bei der Tastatur und dem Bildschirm sehr ins Gewicht. Da der Benutzer auf diese Geräte unmittelbar angewiesen ist, machen sich Unterschiede in der Bauform insofern bemerkbar, als das Arbeiten an Tastatur und Bildschirm über längere Zeiten mehr oder weniger stark ermüdend bzw. anstrengend sein kann.

4.1.1.1.1. Tastaturbereiche

Jede Computertastatur lässt sich grob in fünf Bereiche unterteilen, wobei die Übergänge von einem Block zu einem anderen konstruktionsmäßig auch fließend sein oder einzelne Blöcke sogar fehlen können:

1. Alphanumerischer Block
2. Ziffern - Block
3. Cursor - Block
4. Funktionstasten
5. Spezialtasten

Der alphanumerische Block ist im Wesentlichen bei allen Computertastaturen gleich. Unterscheidungen gibt es hinsichtlich der Anordnung der Tasten, es ist die deutsche DIN möglich, auch QWERTZ-Anordnung genannt oder die amerikanische ASCII, auch QWERTY-Anordnung genannt.

Daneben gibt es noch weitere andere nationale Tastaturen, die alle eine spezielle Tastenanordnung aufweisen.

Die häufig beim Kauf eines Computers mitgelieferte Software beinhaltet meistens ein oder mehrere Programme, die die Tastatur auf verschiedene Bedürfnisse, z. B. die entsprechende Nationalität anpasst. Dabei ist jedoch zu beachten, dass nicht nur nationale Zeichen gegen andere ausgetauscht werden, sondern vielfach auch die „Lage“ der Tasten verändert wird.

Das Betriebssystem MS-DOS erlaubt die Umschaltung zwischen dem amerikanischen und dem gewählten nationalen Zeichensatz. Entspricht die Tastatur dem nationalen Zeichensatz, so kann durch gleichzeitiges Drücken von STRG - Taste, Alt - Taste und F1 der amerikanische und umgekehrt durch gleichzeitiges Drücken von

STRG - Taste, Alt - Taste und F2 der nationale Zeichensatz aktiviert werden.

So wird z. B. die Zeichenfolge ”üüü” nach Umschaltung auf den amerikanischen Zeichensatz zu ”[[[”. Man beachte, dass nicht nur Zeichen, sondern mehrere Tasten der Tastatur vertauscht werden.

Ein externer oder zusätzlicher Ziffernblock (manchmal auch liebevoll „ALDI-Block“ genannt) ist im Prinzip nur dann von Vorteil, wenn Anwenderprogramme vorhanden sind die viele Zahleneingaben verlangen. Vorteilhaft ist es, wenn der Ziffernblock um die mathematischen Zeichen ”+-*/.,” erweitert ist (Abb. 1).

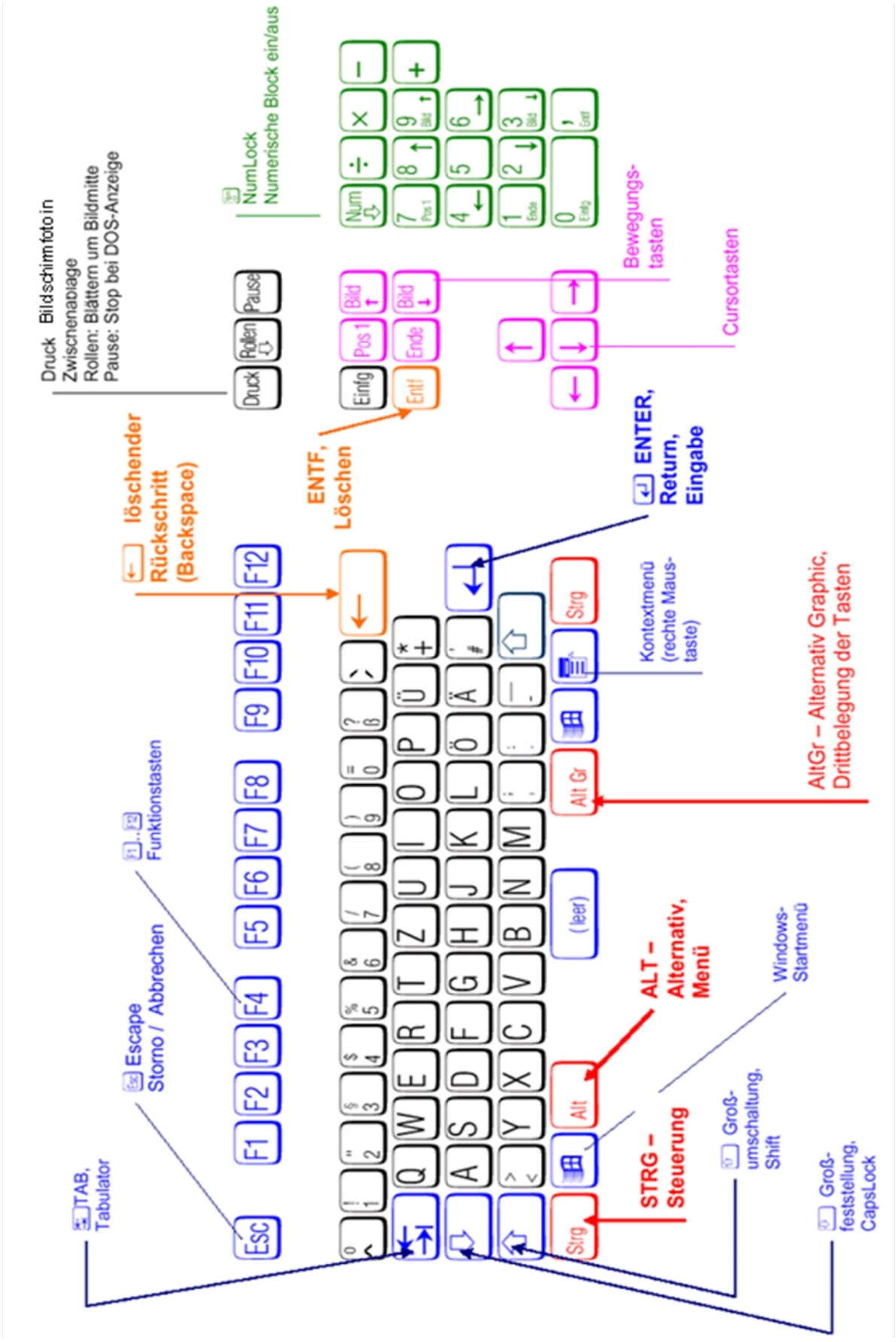
Funktionstasten erleichtern das Arbeiten mit Anwenderprogrammen, denn sie können mit einem bestimmten Code (Text) belegt werden, der über eine normale Zeicheneingabe hinausgeht. Die meisten Tastaturen verfügen über 10 Funktionstasten, F1 bis F0, es gibt aber auch Ausführungen mit bis zu 30 und mehr.

Die Cursor-(Pfeil-)Tasten erlauben z. B. das Springen innerhalb eines Textes bei der Textverarbeitung. Sie werden relativ häufig benutzt, sollten deshalb auch nach Möglichkeit in einem gesonderten Block vorhanden sein. Neben den vier Funktionen ”Hoch”, ”Tief”, ”Links” und ”Rechts” gibt es standardmäßig noch die ”Home” - Taste, die ein Springen in die linke obere Ecke des Bildschirms ermöglicht. Häufig sind die Cursor - Tasten in den Ziffernblock integriert, was zwar Platz spart, aber nicht unbedingt benutzerfreundlich sein muss.

Zu den so genannten „Spezialtasten“ zählt insbesondere die ENTER-Taste, auch RETURN-Taste genannt.

Fast alle Eingaben müssen mit dieser Taste bestätigt werden. Für ein gutes Arbeiten empfiehlt es sich daher, dass die ENTER-Taste mindestens die Größe von drei normalen Tasten aufweist, damit sie leicht und sicher betätigt werden kann. Besitzt die Tastatur einen isolierten Ziffernblock, sollte hier eine zusätzliche Enter-Taste, wenn auch in kleinerem Format, angebracht sein.

4.1.1.1.2. Das Tastaturschema



4.1.1.1.3. Technische Merkmale

Tastaturen können rein mechanisch oder/und elektronisch (elektrisch) aufgebaut sein. Die derzeit verwendeten Computertastaturen arbeiten vielfach nach dem kapazitiven Prinzip (Sensortechnik), d.h. rein elektronisch; die Mechanik ist nur für den Tastenweg verantwortlich.

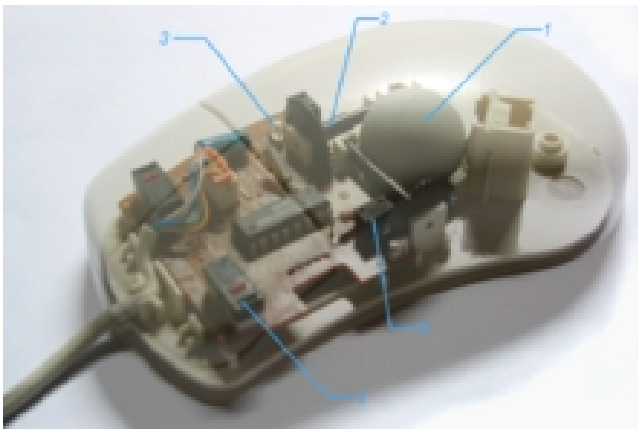
4.1.1.2. Die Maus

Die Maus ist eines der wichtigsten Eingabegeräte (Befehlsgeber) bei modernen Computern. Die Entwicklung von grafischen Benutzeroberflächen hat von der Verfügbarkeit dieses gebräuchlichen und heute weit verbreiteten Zeigegerätes (engl.: Pointing Device) stark profitiert.

Die Bewegung der Maus (normalerweise mit der Hand) auf dem Tisch oder einer speziellen Unterlage, dem Mauspad, wird über einen Sensor in der Maus aufgenommen, digitalisiert und über eine Schnittstelle an den angeschlossenen Computer übertragen.

Über Funktionen des Betriebssystems wird diese zweidimensionale Bewegungsinformation in eine gleichartige Bewegung des Mauszeigers (fälschlicherweise umgangssprachlich auch Cursor genannt) auf dem Bildschirm umgesetzt. Durch Betätigung der Tasten oder zusätzlicher Elemente der Maus kann der Nutzer verschiedene Aktionen in dem Betriebssystem oder Anwendungsprogramm durchführen.

Die Bedienung der Maus kann über das Betriebssystem für Links- bzw. Rechhänder individuell angepasst werden. Einige Mäuse lassen sich jedoch aufgrund ihrer Bauform nur von Link- oder Rechtshändern bedienen.



Innenansicht: 1. Maus-Kugel, 2. Lochscheiben, 3. LED (Lichtquelle der Lichtschranke), 4. Taster, 5. Optischer Sensor (Empfänger der Lichtschranke)

Man kann verschiedene Verfahren zur Aufnahme der Mausbewegung unterscheiden.

4.1.1.2.1. Mechanisch-Elektrisch

Die ersten Mäuse funktionierten mit mechanischen Kontakten: in der allerersten Generation der Computermäuse wurden noch Schleifkontakte zur Koordinatenermittlung verwendet, welche jedoch starkem Verschleiß unterlagen.

4.1.1.2.2. Optomechanisch

Funktionsdarstellung einer optomechanischen Maus:
1: Bewegen der Maus erzeugt Drehung der Kugel.
2: X- und Y-Achsen übernehmen den jeweiligen Anteil der Bewegung.
3: Lochscheiben werden gedreht.
4: Infrarot-LEDs leuchten durch die Lochscheiben.
5: Sensoren empfangen Lichtimpulse, die in X- und Y-Geschwindigkeiten umgesetzt werden.

Heute noch sind optomechanische Mäuse üblich, bei denen die Mausbewegungen über eine Rollkugel, zwei Lochscheiben und zugehörige Lichtschranken in elektrische Signale umgewandelt werden. Die Rollbewegung der Kugel wird über zwei Walzen auf zwei gelochte Segmentscheiben übertragen, aus deren Drehrichtung und Geschwindigkeit werden über Inkrementalgeber mit kleinen Lichtschranken elektrische Impulse erzeugt.

Die relativen Koordinaten zur Darstellung des Mauszeigers werden im Computer mit einer entsprechenden Software (Maustreiber) errechnet.

Kugelmäuse sind anfällig für Verschmutzung, da die Kugel aus Vollgummi immer wieder Partikel in das Mausinnere zieht und diese Partikel der Mechanik, Optik und Elektronik mit der Zeit anhaften, was die Präzision der Maus vermindert.

Auch soll es vorkommen, dass durch Lichteinfall in nicht lichtdicht verschlossene Mausgehäuse die Lichtschranken eine (nicht vorhandene) Bewegung aufnehmen und den Mauszeiger sprunghaft über den Bildschirm wandern lassen. Vorteilhaft gegenüber optischen Mäusen mit dem bildverarbeitenden Prozessor macht sich ein reduzierter Strombedarf bemerkbar (25 mA vs. 100 mA bei einer optischen Maus).

4.1.1.2.3. Optisch mit Leuchtdioden

Neuere Mausgenerationen beleuchten die Oberfläche, auf der die Maus bewegt wird, mit einer eingebauten Lichtquelle (typischerweise mit einer Leuchtdiode) und nehmen die Reflexionen mit einem optischen Sensor auf. Ein eingebauter Mikroprozessor berechnet aus den Unterschieden zwischen nacheinander aufgenommenen Bildern Richtung und Geschwindigkeit der Bewegung der Maus. Man nennt diese Art optische Maus. Ausfallerscheinungen durch verschmutzte Kugeln und vor allem Rollachsen können konstruktionsbedingt nicht

mehr auftreten. Da abgesehen von den Tasten keine mechanisch bewegten Teile mehr vorhanden sind, arbeiten solche Mäuse sehr zuverlässig.

Die ersten Mäuse dieser Art benötigten spezielle Mauspads, auf denen ein Gitter oder Punkte aufgezeichnet waren, an denen sich der optische Sensor orientieren konnte (System von Steve Kirsch, Mouse Systems). Mit höherer Leistung der in den Mäusen verbauten Mikroprozessoren können heute rechenintensivere Algorithmen zur Bildverarbeitung eingesetzt werden. So funktionieren moderne optische Mäuse auf fast allen Unterlagen. Nur Flächen, die eine sehr geringe oder keine Struktur aufweisen, z. B. Spiegel, Glas und viele lackierte Flächen, sind prinzipbedingt ungeeignet. Die hohe Präzision moderner optischer Mäuse macht sich besonders in grafischen Anwendungen und in Computerspielen positiv bemerkbar.

4.1.1.2.4. Optisch mit Laserdioden

Die Lasermaus stellt eine verbesserte Variante der optischen Maus dar. Dabei wird statt der normalen Leuchtdioden eine Laserdiode als Lichtquelle eingesetzt. Dies ergibt durch den Speckleeffekt (ein einzelner Lichtfleck innerhalb eines Musters) einen besseren Kontrast auch auf sehr glatten Oberflächen, transparente Oberflächen bleiben jedoch problematisch. Die Laserdiode verbraucht aufgrund einer gepulsten Betriebsweise weniger Energie als die Leuchtdiode einer optischen Maus, wodurch längere Batteriestandzeiten bei kabellosen Mäusen möglich sind.

Empfindlichkeit

Je nach verwendetem Bewegungsaufnehmer (mechanisch-elektrisch, optomechanisch, optisch mit LED oder Laser-Leuchtdiode) richtet sich die Empfindlichkeit der Maus, d.h. die Strecke, die auf der Unterlage mit der Maus verfahren werden muss, um eine bestimmte Strecke mit dem Mauszeiger auf dem Bildschirm zurückzulegen. Dabei resultiert eine hohe Empfindlichkeit in einem kurzen Verfahrweg auf der Unterlage. Einfluss hat darauf die manchmal bei Mäusen angegebene Auflösung in dpi, je mehr Punkte auf einer bestimmten Strecke aufgelöst werden können, desto empfindlicher ist die Maus.

Manche Betriebssysteme bieten die Möglichkeit, die Empfindlichkeit individuell zu beeinflussen. Neuerdings ist die Beschleunigung im Betriebssystem einstellbar, wenn zusätzlich zur zurückgelegten Strecke die Dauer der Bewegung ausgewertet wird. Bei Bewegung auf großen Flächen ist es hilfreich, wenn die große Strecke mit einer schnellen Bewegung überwunden werden und die genaue Annäherung an den gewünschten Punkt (das Zielen) dann mit normaler Geschwindigkeit erfolgen kann.

4.1.1.2.5. Kabellose Mäuse

Kabellose Mäuse übertragen ihre Informationen nicht mehr durch das manchmal störende Kabel. Stattdessen werden die Daten von der Maus via Infrarot oder Funk (beispielsweise Bluetooth oder in einem anderen ISM-Band; etwa 27 MHz) zu einer Basisstation übertragen,

die das Signal dann per Kabel über die serielle, PS/2- oder eine USB-Schnittstelle an den Computer weiterleitet.

Kabellose Mäuse benötigen eine eigene Stromversorgung, etwa durch Batterien oder Akkus. Zum Nachteil des höheren Gewichtes kommt hier die Notwendigkeit des Batteriewechsels oder Nachladens. Weiter können kabellose Mäuse meist relativ leicht „abgehört“ werden und haben oft eine längere Reaktionszeit. Es sind auch kabellose Mäuse ohne interne Stromversorgung verfügbar, die über Induktion von einem speziellen mitgelieferten, an einem USB-Anschluss angeschlossenen Mauspad mit Energie versorgt werden.

4.1.1.3. Der Trackball

Ein Trackball (auch: Track Ball, deutsch Rollkugel) ist ein Eingabegerät, das aus einem Gehäuse besteht, in dem eine Kugel angebracht ist. Die Kugel wird mit den Fingern bewegt. Im Gehäuse erfassen optomechanische oder optische Sensoren die Bewegung der Kugel entlang zweier Achsen.

Im Desktop-Bereich werden heutzutage Trackballs weitgehend mit den gleichen Sensoren wie optische Mäuse ausgerüstet, im industriellen Bereich werden beide Techniken in etwa gleichem Maße eingesetzt. Der Trackball funktioniert wie eine Art auf den Kopf gelegte Computermaus. Gehäuse und Kugel bestehen üblicherweise aus Kunststoff.

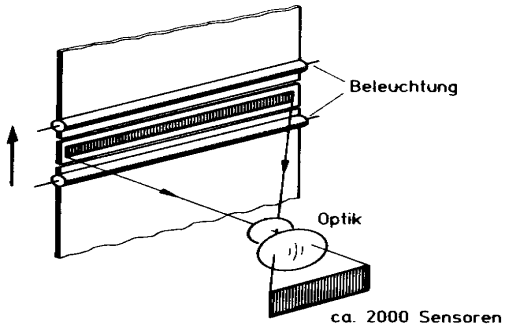
Trackballs werden in verschiedenen Bauformen hergestellt. Bei der gängigsten ist die Kugel am oberen Ende eines mehr oder weniger rechteckigen Gehäuses angebracht und wird mit dem Zeigefinger oder auch anderen Fingern bewegt. Die Maustasten befinden sich symmetrisch links und rechts neben der Kugel. Diese Variante kann von Rechts- wie Linkshändern gleichermaßen benutzt werden.

4.1.1.4. Der Scanner

Scanner werden benutzt, um vorhandene Vorlagen, Texte oder Bilder im Rechner verarbeiten zu können. Die entsprechenden Vorlagen werden durch Fotoelemente abgetastet und ihre Hell-Dunkel-Werte in digitaler Zahlenform '0' oder '1' gespeichert.

Da das abgestrahlte Licht von hellen und dunklen Flächen unterschiedlich reflektiert wird, wird die reflektierte Strahlung auf eine fotoempfindliche Zeile mit circa 2000 Sensorelementen gebündelt.

Im Laufe der Zeit haben sich verschiedene Arten von Scannern etabliert. Zu den bekanntesten gehört der Flachbettscanner. Beim Flachbettscanner wird die Vorlage mit der Bildseite nach unten auf eine Glasfläche aufgelegt.



Die Sensorenzeile und Lichtquelle befinden sich unter der Glasplatte und werden beim Scannen in Längsrichtung bewegt. Beim Einzugsscanner wird die Vorlage über ein Walzensystem an der feststehenden Sensorenzeile vorbeigeführt.

4.1.1.5. Spezialisierte Eingabegeräte

Auf dem Sektor der Eingabegeräte nehmen Tastatur und Maus wegen ihrer Vielseitigkeit den größten Raum ein. Aber es gibt auch eine ganze Reihe von Spezialisten. Einige davon arbeiten nach dem gleichen Prinzip wie Mäuse. Sie ermöglichen dem Anwender, die Cursorposition auf dem Bildschirm auf der Grundlage eines Gitters mit horizontalen und vertikalen Koordinaten zu bestimmen und dann verschiedene Funktionen mit geräteeigenen Schaltern oder Knöpfen auszuwählen und aufzurufen.

Zu dieser Kategorie gehört auch der Lichtgriffel, mit dem direkt auf dem Bildschirm gezeichnet und auch dort gelöscht werden kann. Ein anderes Zeichengerät ist das Graphiktablett, das oft bei der Erstellung technischer Zeichnungen eingesetzt wird. Es besteht aus einer rechteckigen Arbeitsfläche auf der die Bildschirmkoordinaten aufgetragen sind und arbeitet als Radiosender. Der zugehörige Stift dient als Empfänger.

Verwendung eines Lichtgriffels an einem Computerterminal, 1969

Ein drucksensitiver Bildschirm (Touchscreen, Tastschirm bzw. Sensorbildschirm) ist ein besonders konstruierter Monitor, der sowohl Ausgabe- als auch Eingabefunktion hat.

Bei einigen Modellen besteht die Oberfläche aus zwei dünnen, übereinander liegenden Kunststofffolien, die unsichtbare feine Drähte enthalten. Die Anordnung der Drähte entspricht der Matrix einer Tastaturplatine. Als Antwort auf Eingabeaufforderungen, die auf dem Bildschirm erscheinen, wählt der Anwender sowohl Koordinaten als auch Funktionsschalter unmittelbar durch Antippen mit dem Finger. Der leichte Druck reicht aus, um an bestimmten Kreuzungspunkten der Matrix einen Kontakt zu schließen und so Befehle und Daten zur weiteren Verarbeitung an den Computer zu leiten. Die technische Umsetzung der Befehlseingabe ist für den Nutzer quasi „unsichtbar“ und erzeugt so den Eindruck einer unmittelbaren Steuerung eines

Computers per „Fingerzeig“. Das durch den Touchscreen „berührungsempfindliche“ Bild kann dabei sowohl dynamisch mittels Monitor oder über Projektion, als auch physikalisch (z. B. gedruckt) generiert worden sein. Touchscreens finden als Info-Monitore, z. B. auf Messen, zur Orientierung in großen Kaufhäusern oder für die Fahrplanauskunft auf Bahnhöfen Verwendung. Hin und wieder sind auch in den Schaufenstern von Apotheken oder Reiseveranstaltern Touchscreens zu finden, über die detaillierte Informationen abgerufen werden können. Darüber hinaus werden Touchscreens auch bei Spielautomaten und Navigationsgeräten eingesetzt.

So wie optische Scanner Bildpunkte umwandeln, können Sound Digitizer akustische Signale wie beispielsweise Sprache oder Musik in Zahlen umwandeln. Unabhängig von der Art der Schallquelle müssen die Töne erst in ein elektrisches Signal umgeformt werden. Dies erfolgt gewöhnlich durch ein Mikrophon oder einen Tonaufnehmer an einem Musikinstrument. Das Signal wird von einem schnellen AD - Wandler mit einer Frequenz von gewöhnlich 44.000 Hertz gesamplet und in Bits und Bytes verwandelt. Dieser Technologie verdanken wir die Compact Disc mit der ganzen Reinheit ihres Klanges. Die für CD-Aufnahmen benutzten Verfahren werden bei Computern auch für optische Massenspeicher benutzt.

Selbst die Digitaltelefone sind Eingabegeräte, weil auch sie mit Computeranlagen in Verbindung stehen. Jede Taste des Telefons erzeugt einen hörbaren Ton einer bestimmten Frequenz. Wenn die Töne in der computerisierten Telefonvermittlung in numerische Werte umgewandelt worden sind, geben sie dem Computer Anweisungen, wohin der Anruf geschaltet werden soll. PC können so ausgestattet werden, dass sie die Töne in Anwendungen wie Gebäudesicherungsanlagen umformen können – der Anwender kann dann den verschiedenen Untersystemen (wie z. B. der Beleuchtung, der Alarmsicherung oder Türanlagen) telefonisch Anweisungen erteilen.

Der Strichcodeleser (auch Barcodeleser) an der Kasse eines Supermarktes ist ein Eingabegerät, das viele seiner spezialisierten Fähigkeiten im Verborgenen entfaltet.

Es ist ein Datenerfassungsgerät, das verschiedene Barcodes lesen und weitergeben kann. Die Erkennung dieser Strichcodes erfolgt dabei rein optisch entweder mit Rot- oder Infrarotlicht.

Jeder Barcodeleser besteht aus der eigentlichen Leseeinheit und der nachgeschalteten Dekodiereinheit. Den Informationsrohstoff für den Computer des Supermarktes liefern die Waren in den Regalen.

Auf jeder Packung im Laden ist ein Muster von Strichen und Zwischenräumen angebracht, das in Europa als EAN-Code (”Europaeinheitliche Artikelnummer”) bezeichnet wird. Ein breiter Strich oder Zwischenraum steht für eine Eins, ein schmaler Strich oder Zwis-

chenraum für eine Null. Wenn die Packung über das Lesegerät geschoben wird, erzeugt ein Laserstrahl im Gerät ein Netz von Infrarotstrahlen mit dem der Strichcode abgetastet wird. Striche und Zwischenräume unterbrechen die Strahlen und wenn diese in den Mechanismus reflektiert werden, liest der Scanner die Unterbrechungen als binäre Einsen und Nullen.
Diese Information wird vom Computer des Supermarktes verarbeitet, der seine Ergebnisse an mehrere Bestimmungsorte schickt. Einer davon ist die Registrierkasse, wo sie als erleuchtete Anzeige des Preises und als Ausdruck auf dem Bon erscheinen, manchmal noch zusätzlich als körperlose, mechanische Stimme, die jeden gekauften Gegenstand benennt.

Die Daten werden auch an das computerisierte Warenbestandsverzeichnis des Supermarktes weitergeleitet. Wenn der Lagerbestand eines beliebigen Artikels unter einen bestimmten Wert sinkt, bestellt der Computer automatisch neue Ware.

Barcode

Der Computer dirigiert die vom Strichcodeleser generierten Eingabedaten vielleicht sogar zu einem vorprogrammierten Marketingservice, der auf die individuellen Kaufgewohnheiten eines jeden Kunden zugeschnittene Gutscheine für preisreduzierte Ware ausdruckt. Kauft der Kunde beispielsweise mehrere Gläser Spaghettisauce, könnte auf dem Gutschein ein Sonderangebot für eine bestimmte Marke Parmesankäse ausgewiesen werden.

Auf dem Prinzip der virtuellen Realität beruhende Geräte wie Sensorhandschuhe, Sensoranzüge und 3D - Brillen, die früher den Exoten zuzurechnen waren, werden allmählich immer mehr zu ganz normalen Eingabegeräten. Mit ihnen kann der Anwender sozusagen am eigenen Leib die künstliche Rekonstruktion einer Realität erfahren, die für ihn von der tatsächlich vorhandenen Welt nahezu nicht zu unterscheiden ist oder auch von völlig imaginären Welten.

Arbeitet etwa ein Architekt nach diesem Prinzip, so kann er sich durch perspektivische Ansichten eines Gebäudes bewegen, als würde er durch die Räume gehen und das, bevor der Bau überhaupt errichtet ist. Der Pilot eines Jagdflugzeuges kann mit all seinen Sinnen jeden Sekundenbruchteil eines Luftkampfes erleben, ohne dabei festen Boden verlassen zu müssen. Jede seiner Reaktionen auf die simulierte Kampfsituation wird zur Eingabe in das System. Egal ob er eine Kurve fliegt oder in den Steigflug übergeht, sich in Feuerposition bringen oder den Kampf abbrechen will - jede seiner Entscheidungen wird durch die Betätigung der Ruder an den Computer übermittelt. Der Computer meldet die Ergebnisse dieser Entscheidungen verzögerungsfrei an den Piloten zurück. Die Instrumente, die er erblickt und die Geräuscheffekte, die er hört, sind ebenso ein Teil seiner scheinbar realen Umgebung wie die Flugbewegungen, die die hydraulische Mechanik des Simulators erzeugt.

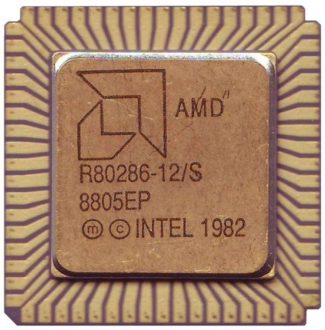
Die Eingabe in einen Computer kann ein bewusst vorgenommener, vom Anwender genau überlegter Schritt sein; etwa die Entscheidung, an einem Bankautomaten einen bestimmten Befehl auszuwählen oder ein Wort aus einem Textabschnitt zu löschen. Es kann sich aber auch um einen im Hintergrund ablaufenden, nicht wahrnehmbaren Prozess handeln, der von automatischen Eingabegeräten erfasst und in Form von Bewegungs- oder Temperaturmesswerten, umgewandelt in Datenbits, der CPU zugeleitet wird.

Eingabedaten können so unterschiedliche Größen sein wie ein Wort, ein Temperaturwert, eine Hirnabtastung, eine Photographie oder der Preis für ein Pfund Kaffee - für einen Computer besteht kein Unterschied. Die CPU unterscheidet nicht zwischen Bildern, Zahlen oder Tönen. Wenn auch der Eingabeprozess selbst ohne Verzögerung abzulaufen scheint, ist doch eine Anzahl von Schritten abzuarbeiten. Sofern die Rohdaten eingegeben und auf dem Weg über die Eingabeports und die CPU im Speicher abgelegt worden sind, haben sie die Umwandlung in binäre Zahlen hinter sich, in die einzige mathematische Sprache, die die CPU verstehen und manipulieren kann. Erst wenn der Computer die Daten auf diesem Weg erhalten hat, ist er bereit, den nächsten wichtigen Schritt durchzuführen: sie zu verarbeiten.

4.1.2. Verarbeitungsgeräte

Kernstück jedes PC's ist die Zentraleinheit. Sie koordiniert alle Operationen, sämtliche Komponenten des Systems, ruft Programmbefehle ab und führt sie aus, transportiert Daten auf elektronischen Verbindungswegen. Die Zentraleinheit berechnet alle arithmetischen und logischen Operationen, die im Rahmen der jeweils gestellten Aufgabe anfallen. Speicherbanken unterstützen die elektronische Verarbeitungskapazität, während ein interner Taktgeber als Schrittmacher dient und elektrische Impulse erzeugt, mit denen die Millionen von geforderten Entscheidungen synchronisiert werden.

Die zwei Hauptteile der Zentraleinheit sind der eigentliche (Haupt-)Prozessor (CPU = Central Processing Unit) selbst und der interne Speicher.



Diese können wiederum unterteilt werden:

- der Prozessor in das
  - Rechenwerk
  - Steuerwerk

und

- der interne Speicher in einen
  - nichtflüchtigen Speicher (ROM)
  - einen flüchtigen Speicher (RAM)

Aufgaben der einzelnen Komponenten:

Bei der Verarbeitung im Inneren des Computers geht es in vielerlei Hinsicht ähnlich zu wie auf einem Rangierbahnhof: der Fracht wird aus Güterwagen entladen, neu zusammengestellt. Damit wird ein neuer Güterwagen beladen. Es wird eine neue Zugzusammenstellung vorgenommen und es erfolgt der Weitertransport zum Zielort.
Koordination aller Aktionen ist das oberste Gebot!

4.1.2.1. Steuerwerk

Das Steuerwerk lenkt und koordiniert den Gesamtablauf entsprechend dem Arbeitsprogramm. Es entnimmt die Befehle aus dem Speicher, interpretiert sie und steuert die Befehlsausführung.

4.1.2.2. Rechenwerk

Das Rechenwerk führt die arithmetischen (addieren, subtrahieren) und logischen (UND-, ODER-, NICHT-) Operationen durch.

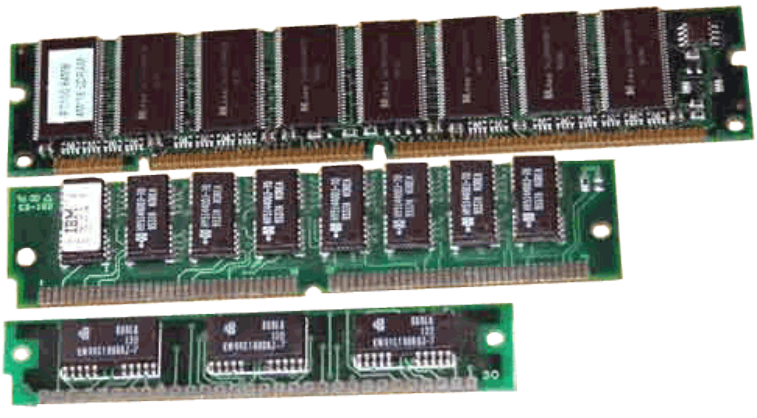
4.1.2.3. Interner Speicher

Der interne Speicher speichert Programme oder Programmteile, nimmt zu bearbeitende Daten auf und leitet sie an den Prozessor weiter, übernimmt dessen Ergebnisse und gibt sie nach außen ab.

Aufgaben der internen Speicher:

- Unter dem **ROM** (engl. READ-ONLY-MEMORY) Speicher versteht man einen Datenspeicher, der nur lesbar ist, im normalen Betrieb aber nicht beschrieben werden kann und nicht flüchtig ist, das heißt: er hält seine Daten auch in stromlosem Zustand. Das prädestiniert ihn zur Aufnahme von „fest verdrahteten“ Computerprogrammen wie z. B. dem BIOS1. Er enthält alle Programmteile, die zur Organisation innerhalb der Zentraleinheit nötig sind. Typische Aufgaben des ROM sind zum Beispiel Routinen zum Selbsttest des Rechners und dessen Meldung nach dem Einschalten, dass nun Daten eingegeben werden können.

- Im **RAM** (engl. RANDOM ACCESS MEMORY; dt.: Speicher mit wahlfreiem Zugriff) Speicher können Programme und Daten eingelesen und dem Prozessor zur Verarbeitung weitergegeben werden. Allerdings speichert der RAM - Speicher die Daten und Programme nur so lange, wie er mit Strom versorgt wird. Mit dem Ausschalten des PC sind alle nicht gesicherten



Daten unwiederbringlich verloren. Ebenso, wenn der Rechner während der Arbeit plötzlich nicht mehr reagiert. Er ist dann abgestürzt und die Daten sind verloren. Der Datenverlust beschränkt sich jedoch auf die Daten, die nur im Arbeitsspeicher sind. Daten die bereits auf der Festplatte gespeichert wurden, stehen noch zur Verfügung.

4.1.3. Ausgabegeräte

4.1.3.1. Monitor

Der Monitor ist das Fenster zum Rechner. Das System Grafikkarte/Monitor ist die wichtigste Schnittstelle zwischen dem Rechner und seinem Anwender. Beim Computerkauf kommt der Monitor jedoch meistens zu kurz. Der Monitor ist häufig die teuerste Komponente am Rechner, so dass hier am drastischsten der Preis gedrückt werden kann. Was aber nimmt der Anwender für ein paar gesparte Euro in Kauf? Er ruiniert sich durch langen Gebrauch eines schlechten Monitors unter Umständen seine Gesundheit, vor allem die der Augen.

Niemand sollte sich daher mit dem Argument abspeisen lassen, dass ein kleiner Monitor ausreicht, wenn der PC vor allem zur Textbearbeitung genutzt wird. Moderne graphische Oberflächen machen den Bildschirm nicht nur zum Ausgabegerät, sondern im Zusammenspiel mit der Maus auch zum wichtigen Eingabegerät. Bei kleineren Monitoren nehmen Kontrollelemente einen großen Teil der sichtbaren Fläche ein, so dass kaum Platz für die eigentliche Arbeitsfläche bleibt.

Vorgeschrieben ist mindestens ein 17-Zoll-Monitor, mit dem sich die Möglichkeiten von Betriebssystemen wie Windows, Macintosh oder OS/2 erst sinnvoll ausnutzen lassen. Die Vergrößerung der Bildschirmdiagonalen um fünf Zentimeter (17 Zoll anstelle von 15 Zoll) bedeutet aber eine Ausweitung der sichtbaren Fläche um 30 Prozent. Dennoch ist die Farbgestaltung auch bei Farbmonitoren nicht beliebig einsetzbar. In diesem Zusammenhang fällt oft der Begriff der Negativ- bzw. Positivdarstellung. Die Darstellung von dunklen Buchstaben auf hellem Grund ist die so genannte Positivdarstellung. Diese Einstellung sollte ausschließlich gewählt werden, damit die Belastung der Augen durch minimale Anpassungen möglichst gering gehalten wird.

Ich bin ein Text, der manchmal nur schwer lesbar ist. Das liegt daran, daß ich manchmal mit weißer Schrift auf dunklem Grund stehe. Stehe ich mit schwarzer Schrift auf hellem Grund, bin ich sehr gut zu lesen.
Ich bin ein Text, der manchmal nur schwer lesbar ist. Das liegt daran, daß ich manchmal mit weißer Schrift auf dunklem Grund stehe. Stehe ich mit schwarzer Schrift auf hellem Grund, bin ich sehr gut zu lesen.

Negativdarstellung *Positivdarstellung*

Computermonitore arbeiten wie alte Fernsehgeräte nach dem System der Braunschen Röhre, die im englischen Cathode Ray Tube (CRT) genannt wird.

4.1.3.2. LCD Bildschirme

Vorteile der LC - Displays sind, dass sie energiesparend sind. Sie verbrauchen maximal 20 Watt im Gegensatz zu mehreren hundert bei herkömmlichen Röhren.

Von den Displays geht keine Strahlung aus, das geringe Gewicht und die Größe sind weitere Vorteile. Hinzu kommt, dass keine Verzerrungen durch die Wölbung, wie es sie bei den Röhrenbildschirmen gibt, auftreten.

Nachteile sieht man in dem großen Aufwand um diese Displays mit einer guten Qualität herzustellen und damit den hohen Anschaffungspreis.

Unter den Flachbildschirmen am weitesten verbreitet ist die durch Digitaluhren und Taschenrechner bekannte Flüssigkristalltechnik. Die Abkürzung LCD bezeichnet kurz das physikalische Prinzip und steht für Liquid Crystal Display, auf deutsch Flüssigkristallanzeige. Eine Weiterentwicklung ist das Aktiv-Matrix-Display, das zur Ansteuerung eine Matrix von Dünnschichttransistoren (engl. thin film transistor, TFT) enthält.

Bei Flachbildschirmen ist diese Technik seit Ende 2007 vorherrschend. LCDs finden Verwendung an vielen elektronischen Geräten, etwa in der Unterhaltungselektronik, an Messgeräten, Mobiltelefonen, Digitaluhren und Taschenrechnern. Auch Head-Up-Displays und Videoprojektoren arbeiten mit dieser Technik.

4.1.3.3. Drucker

4.1.3.3.1. Nadeldrucker

Ein Nadeldrucker gehört wie sein Vorgänger, der Typenraddrucker, zu den Impact-Druckern. Da die Zeichen mittels einer Matrix erzeugt werden, zählt er wie auch der Tintenstrahldrucker zu den Matrixdruckern. Beim Druckvorgang schlagen einzeln durch Magneten angesteuerte Nadeln (8, 9, 12, 18, 24 oder 48 Stück) auf ein Farbband zwischen Papier und Druckkopf, wodurch die Bildpunkte

abgebildet werden, aus denen sich
die Zeichen zusammensetzen.

Je höher die Anzahl der Nadeln ist, desto enger können die Punkte gesetzt werden und desto besser wird das Druckbild. Mit dieser Technik erreicht man je nach Typ und Druckqualität eine Druckgeschwindigkeit von bis zu 1000 Zeichen pro Sekunde (CPS).

Im Entwurfsmodus (engl. Draft-Modus) wird der Druckkopf mit hoher Geschwindigkeit bewegt. Die Nadeln werden dabei in einer groben Matrix zeilenweise angesteuert. Das Schriftbild ist dadurch nur zweckmäßig lesbar. Oft wird hierbei eine Schriftart mit einem Raster von nur 8 x 9 Punkten verwendet, auch wenn der Drucker über 24 oder gar noch mehr Nadeln verfügt. Die Geschwindigkeit des Ausdrucks ist dadurch jedoch sehr hoch. Typisch sind ca. 200-400 CPS.
Der NLQ-Modus (Near Letter Quality, zu deutsch: nahezu Korrespondenzqualität) wird bei einem Nadeldrucker verwendet, um die Druckauflösung zu verbessern. Der Druckkopf fährt dabei nur mit halber Geschwindigkeit, was eine Verdopplung der waagerechten Auflösung bedeutet. Er druckt alle Zeichen der Zeile. Am Ende der Zeile erfolgt ein Zeilenvorschub um ½ Nadeldurchmesser und die Zeile wird erneut gedruckt. Somit sind die Zwischenräume des Druckbildes nun ebenfalls aufgefüllt (Senkrechte Auflösung). Ein Ausdruck benötigt in diesem Modus bis zu viermal mehr Zeit. Eine mögliche Optimierung bietet hier das bidirektionale Druckverfahren.

Im LQ-Modus (Letter Quality) entspricht das Druckbild einer mit klassischen Verfahren hergestellten Seite, eben „Korrespondenzqualität“. Diese wurde früher zunächst nur von Schreibmaschinen erreicht, deren Qualität sich bis heute durch den Einsatz von Karbonbändern im Vergleich zu ehemals manuell mit Typen angeschlagenen Seidenbändern ebenfalls deutlich verbessert hatte. Heute erreichen handelsübliche Laserdrucker und Tintenstrahldrucker mit Leichtigkeit eine solche Druckqualität. Mit einem Nadeldrucker wird diese Qualität mit einer sehr hohen Horizontalauflösung durch sehr schnelles und präzises Ansteuern der Nadeln erreicht.

Man kann vereinfacht sagen: Je höher die Druckgeschwindigkeit, umso niedriger die Druckqualität.
Während Typenraddrucker kaum noch Verwendung finden, findet man den Nadeldrucker noch häufig in Firmen, da er zuverlässig und robust ist. Nadeldrucker (zunehmend aber auch Thermodrucker) werden zudem in technischen Geräten wie Fahrscheinentwertern, Kaufhauskassen und Parkautomaten verwendet, da sie wenig Wartung erfordern und die Ausdrucke beständig sind.
Der weitaus häufigste Einsatzbereich sind heute noch so genannte Protokolldrucker in großen Firmen oder in Systemen mit hohen Sicherheitsanforderungen. Die einzelnen Protokolle z. B. von Schaltzuständen in Schaltanlagen werden nicht nur digital gesichert, sondern gegen nachträgliche Veränderung immun als sofortiger Ausdruck gefertigt.

Vorteile	Nachteile
• jede Art von Papier bedruckbar • viele Schriftarten und -größen • Drucken mit Durchschlägen möglich • geringe Verbrauchskosten (Farbband) • wartungsarm • verschiedene Druckgeschwindigkeiten • dokumentenecht • verschiedene Druckqualtitäten • kann Endlospapier bearbeiten • wasserfester Ausdruck • hohe Lebensdauer • zeilenweiser Druck möglich • Drucken mit Endlosschleifen	• Lärmbelästigung • geringe Druckgeschwindigkeit • wechselnde Druckqualität (vom Zustand des Farbbandes abhängig) • typisches gerastertes "Computer"-Druckbild • schlechte Farbwiedergabe • hoher Anschaffungspreis • nicht alle Zeichen und Grafiken werden gedruckt • keine Folien bedruckbar • Wärmeentwicklung des Druckkopfes bei Dauerbetrieb

4.1.3.3.2. Tintenstrahldrucker

Tintenstrahldrucker sind Matrixdrucker, bei denen durch den gezielten Abschuss oder das Ablenken kleiner Tintentröpfchen ein Druckbild erzeugt wird. Sie gehören zur Gruppe der Non-Impact-Drucker.
Man unterscheidet zwei Geräteklassen:

- CIJ (Continuous Ink Jet, also Geräte mit kontinuierlichem Tintenstrahl)
- DOD (Drop On Demand, d.h. Geräte die einzelne Tropfen verschießen)

DOD-Drucker findet man sowohl in der Industrie, als auch im Büro- und Heimbereich.

Im Gegensatz zu CIJ-Druckern verlässt hier nur der Tintentropfen die Düse, der tatsächlich gebraucht wird. Die Geräte werden zusätzlich danach unterschieden, mit welcher Technik die Tintentropfen ausgestoßen werden. Der Einsatzbereich ist sehr groß und reicht vom Heim-/Office-Bereich bis zum Druck von Passbildern. Auch elektrische Schaltungen kann man damit aufbauen oder sogar 3D-Modelle z. B. für Rapid Prototyping erzeugen. Anstatt Tinte werden unter anderem Wachs, langkettige Polymere oder heiße flüssige Lote verwendet.

Je nach DOD-Typ wird die Tinte auf eine andere Art aus der Düse getrieben:

Bubble-Jet-Drucker erzeugen winzige Tintentropfen mit Hilfe eines Heizelementes, welches das Wasser in der Tinte erhitzt. Dabei bildet sich explosionsartig eine winzige Dampfblase, die durch ihren Druck einen Tintentropfen aus der Düse presst.

Vorteile	Nachteile
• sehr leise, • gute Geschwindigkeit, • gute Qualität, • niedrige Anschaffungskosten, • Farbdrucker ist meist integriert	• keine Durchschläge möglich, • hohe Druckkosten pro Seite, • teilweise ist für High-Quality-Druck Spezialpapier erforderlich

4.1.3.3.3. Laserdrucker

Der Laserdrucker ist ein Drucker zur Produktion von Ausdrucken auf Papier oder Folien im Laserbelichtungs- und Tonerpartikel-Druckverfahren.

Laserdrucker gehören im Gegensatz zu Nadel- oder Tintenstrahldruckern zu den so genannten Seitendruckern. Die Belichtung und der Druck erfolgen in einem Durchlauf. Im allgemeinen Sprachgebrauch werden auch LED-Drucker meist als Laserdrucker bezeichnet, insbesondere weil das Funktionsprinzip sehr ähnlich ist.

Im Großformat-Bereich wird ebenfalls oft vom Laserplotter gesprochen, obwohl es sich bei allen derzeit verbreiteten Geräten tatsächlich um LED-Plotter handelt. Die Beschichtung wird zunächst elektrostatisch negativ aufgeladen. Entweder mittels einer Ladekorona (ein dünner, nahe der Trommel angebrachter Draht, der unter hohe Spannung gesetzt wird) oder durch Ladungswalzen. Letztere haben gegenüber der Ladekorona den Vorteil, dass kaum noch Ozon produziert wird, weil keine hochspannungsführenden Teile in Kontakt mit der Umgebungsluft stehen.

4.1.3.3.4. Belichtung

Die Ladung auf dem Photoleiter wird nun an den Stellen gelöscht, an denen später kein Toner auf die Trommel aufgetragen werden soll: an den belichteten Stellen wirkt er leitend und verliert dadurch seine Ladung. Zur Belichtung wird ein Laserstrahl über einen rotierenden Spiegel (Laserscanner) zeilenweise auf die Trommel gelenkt und dabei rasterartig an- bzw. Ausgeschaltet.

Grauabstufungen werden bei einfachen Laserdruckern durch Halbtonrasterung erreicht. Entsprechend wird mit weiteren Farben bei einfachen Farblaserdruckern verfahren. Höherwertige Laserdrucker real-

isieren im Vollfarbsystem höhere Auflösungen. Bei ihnen wird die Ladung auf der Trommel nicht in einem Schritt auf Null reduziert, sondern kann in Stufen (bis zu 256) abgeschwächt werden. Erreicht wird die Abschwächung entweder durch unterschiedliche Verweildauer des Lasers an einer Stelle oder durch Mehrfachüberstreichen der entsprechenden Stelle.

4.1.3.3.5. Entwicklung

Der Photoleiter dreht sich weiter und wird in der Entwicklereinheit in unmittelbare Nähe des elektrostatisch gegensätzlich zum Photoleiter negativ aufgeladenen Toner gebracht. Aufgrund der gegensätzlichen Ladung springt der Toner auf die Trommel über und haftet dort an.

4.1.3.3.6. Toner-Transfer

Der Photoleiter bewegt sich weiter und bringt den Toner in Kontakt entweder direkt mit dem zu bedruckenden Medium (Papier) oder zunächst mit einer Transferwalze oder einem Transferband und erst in einem weiteren Schritt auf das Papier.

Beim Mehrfarbdruck werden bei älteren Laserdruckern nacheinander alle Tonerfarben auf das Transfermedium aufgebracht. Um registerhaltig zu bleiben, also die einzelnen Farbauszüge nicht gegeneinander zu versetzen, muss hier besonders präzise positioniert werden. Die Übertragung auf das Papier erfolgt anschließend in einem Schritt für alle vier Farben. Alternativ zum Transfermedium werden auch elektrostatisch vorgeladene Papiertransportbänder (Electrostatic Transport Belt) verwendet, auf denen das Papier wie festgeklebt positioniert werden kann. Bei neueren Geräten besteht der Farb-Laserdrucker aus vier einzelnen Druckwerken (für jede Farbe ein Werk) und das Papier durchläuft alle vier Druckwerke nacheinander. Hier ist eine noch genauere Positionierung des Papiers notwendig. Dieses Druckverfahren bietet aber den Vorteil, dass kontinuierlich gearbeitet werden kann. Während bei alten Geräten mit Transfer-Band das Band immer nur mit einer Farbe beschickt werden konnte (die vier Tonerkartuschen befinden sich in einer Revolver-Trommel und werden nacheinander zum Einsatz gebracht, so dass das Transfer-Band vier Umläufe benötigt, um eine Seite zu vervollständigen), können neuere Geräte mit vier getrennten Druckwerken bereits im ersten Druckwerk die Folgeseite drucken, während das letzte Druckwerk noch damit beschäftigt ist die vorhergehende Seite zu drucken. Dadurch erreichen sie im Farbdruck die gleiche Seitenleistung (Druckseiten / Minute) wie im Monochrom-Druck. Bei den alten Geräten mit Transfer-Band verringert sich beim Farbdruck die Seitenleistung auf 25 % im Vergleich zum Monochrom-Druck.

Der Toner wird dazu gebracht auf das Papier überzuspringen, indem auf der Rückseite des Papiers mittels einer Transferrolle eine starke elektrische Ladung angelegt wird, die wiederum der Ladung des Toners entgegengesetzt ist.

4.1.3.3.7. Fixierung

Das Papier bewegt sich weiter zur Fixiereinheit. Diese besteht im Wesentlichen aus zwei Hohlwalzen, die eine besondere Beschichtung tragen (z. B. Teflon oder Silikongummi). Im Inneren von mindestens einer der zwei Walzen befindet sich ein Heizstab, der die Walze auf rund 180°C (± 10°C, je nach verwendetem Medium) aufheizt. Beim Durchlaufen des Blattes schmilzt der Toner und verklebt mit dem Papier. Dafür, dass möglichst wenig Toner an den Heizwalzen haften bleibt, sorgt einerseits die Beschichtung andererseits wiederum eine entsprechende, leichte elektrostatische Aufladung der Walzen, die den Toner abstoßen (obere Walze) bzw. anziehen (untere Walze, jenseits des Papiers). Der dennoch auf den Heizwalzen verbleibende Toner wird bei höherwertigen Geräten durch Reinigungswalzen oder ein Reinigungsvlies entfernt. Teilweise kommt eine Nassfixierung zum Einsatz, bei der die Heizung über austauschbare Kartuschen mit Silikonöl versorgt wird, welches die ebenfalls vom Benutzer zu tauschenden Reinigungswalzen benetzt. Je nach konstruktivem Aufwand der Fixiereinheiten liegen die Standzeiten im Bereich zwischen 40.000 und 400.000 Druckseiten.

Als einziger Hersteller arbeitet die Firma Océ mit einem Fixierverfahren bei dem eine wesentlich niedrigere Fixiertemperatur (nur rund 70°C) verwendet wird, dafür aber ein wesentlich höherer Druck. Das Verfahren ist konstruktiv aufwendiger und daher so teuer, dass es für Heimanwender-Drucker nicht geeignet ist. Dieses Verfahren hat jedoch den Vorteil, dass auch wärmeempfindlichere Medien bedruckt werden können. Ferner ist bei niedrigeren Temperaturen die Gefahr sehr viel geringer, dass aus den Kunststoffharzen des Toners oder dem Papier selbst schädliche Emissionen austreten.

4.1.3.3.8. Vollentladung

Bei der weiteren Drehung der Trommel wird der verbleibende Resttoner von der Trommel abgestreift. Bei aufwändigeren Konstruktionen wird dieser in einem Resttonerbehälter gesammelt. Dazu wird die Trommel zuerst durch Vollbelichtung entladen. Bei kleineren Geräten mit integrierten Toner-Trommel-Kartuschen wird seit den 90er Jahren der Resttoner zurück in die Developerstation gestreift. Die Grenze zwischen Kleingeräten ohne Resttoneraufangbehälter und Hochvolumendrucker mit Resttonerentsorgung wird sowohl durch die allgemein steigenden Druckleistungen als auch durch technische Entwicklungen vorangetrieben.

Vorteile	Nachteile
• hohe Geschwindigkeit, • sehr gute Qualität, • minimale Lärmbelastung	• keine Durchschläge, • hohe Anschaffungskosten • hohe Betriebskosten, • Bildung von Ozon bei längerer Betriebsdauer

4.1.3.4. Plotter

Ein Plotter (engl. plot = zeichnen), im deutschen auch als Kurvenschreiber bezeichnet, ist ein Ausgabegerät, das Funktionsgraphen, technische Zeichnungen und andere Vektorgrafiken auf verschiedenen Medien darstellt.

Der Stiftplotter ist für Darstellungen auf Papier, in der Regel DIN A3 bis A0 ausgelegt. Dazu benutzt er einen Tuschestift, der auf einem Wagen angebracht ist. Dieser Wagen gleitet über eine Schiene, die entweder über die gesamte Papierbreite verschoben werden kann (Flachbettplotter) oder aber fix montiert ist, während das Papier über eine Walze verschoben wird (Rollenplotter).

Die meisten Plotter arbeiten mit Tuschestiften verschiedener Strichbreiten, die in einem Magazin untergebracht sind und bei Bedarf vollautomatisch am Wagen angebracht werden. Beide Mechanismen erlauben eine schnelle Darstellung von Vektorgrafiken wie einfachen Linien und Kreisen sowie (allerdings recht schmucklosen) Schriftzügen. Stiftplotter finden im gewerblichen Bereich nur noch selten Anwendung.

4.1.4. Speichergeräte / Datenträger

Sämtliche vom Computer benötigten oder verwalteten Daten stehen in diesem nur solange zur Verfügung, wie die Stromversorgung gewährleistet ist. Schaltet man den Rechner aus, so sind sämtliche Daten verloren. Bei Taschenrechnern gilt gleiches, wenn man beachtet, dass man hier mit dem Hauptschalter nur die Stromversorgung für die Anzeigeelemente unterbricht, während die eigentlichen Speicherstellen weiterhin mit Strom aus der Batterie versorgt werden. Ähnliches gilt auch für Digitaluhren. Sobald jedoch die Batterie entfernt wird, sind hier ebenfalls sämtliche Daten verschwunden. Es muss also in jedem Fall dafür Sorge getragen werden, dass die in einem Computer vorhandenen Daten auf einem externen Datenträger dauerhaft, d.h. unabhängig von einer Stromversorgung, gespeichert bleiben.

Die ersten bekannten Datenträger sind die Steintafeln, die bereits vor mehr als 1000 Jahren verwendet wurden. Ein erster wesentlicher Fortschritt erfolgte mit der Herstellung der Pergamentrollen. Man konnte die Datenmenge erheblich vergrößern, da die Handschrift viel weniger Platz benötigte als die eingemeißelten Wörter. Bereits hier wird deutlich, dass man für die ideellen Daten, die Nachricht (engl. Software), immer einen materiellen (engl. Hardware) Datenträger benötigt.

Die ersten bei Computern zur Bedeutung gelangten Datenträger sind die Lochkarten, auch nach ihrem Entwickler Hollerith-Karten genannt. Für spezielle Anwendungsfälle werden sie noch heute verwendet. Die nächste Entwicklungsstufe führte zum magnetischen Datenträger, der Magnetkassette, wie sie vom normalen Kassettenrecorder her bekannt ist. Das Problem bei diesen Magnetbändern besteht darin, dass man Daten, die am hinteren Ende stehen, nur über die davor liegenden erreicht. Dieses Problem ist schon vom normalen Tonband her bekannt. Denn wenn man ein Musikstück sucht, muss man erst alle davor liegenden durchlaufen. Man spricht bei diesem Verfahren auch von sequentieller (gereihter) Datenspeicherung.

Die Verwendung einer magnetischen Scheibe gestattet dagegen, den Tonkopf in größeren Sprüngen zu bewegen, so dass man viel schneller an die benötigten Daten gelangt. Dieses Prinzip, auch wahlfreier Zugriff genannt (engl. Random Access), ist identisch zu einer Schallplatte. Hier kann man das letzte Musikstück direkt erreichen, ohne die davor liegenden erst durchlaufen zu müssen. Die magnetische Scheibe, Diskette oder Floppy-Disk genannt, war bis Mitte der 90er Jahre der am häufigsten verwendete Datenträger für Computerdaten. Dabei sind diese Disketten äußerst empfindlich, denn sie vertragen weder Kälte noch Hitze. Sie haben aber einen entscheidenden Vorteil, sie sind extrem preiswert. Da der Tonkopf direkt auf der magnetischen Schicht der Diskette, die sich mit ca. 100 Umdrehungen/ Minute im Diskettenlaufwerk dreht, aufliegt, ist die Magnetschicht durch den Reibungsvorgang irgendwann zerstört, so dass keine Daten mehr gespeichert werden können.

Von gleicher Wirkungsweise sind die Festplattenlaufwerke. Wie der Name schon erahnen lässt, können sie nicht wie eine Diskette nach Belieben gewechselt werden. Die Festplatten befinden sich in einem hermetisch abgeriegelten Metallgehäuse, welches die sich mit hoher Umdrehungszahl drehenden Magnetplatten vor äußeren Einflüssen schützt. Der Tonkopf ist so aufgebaut, dass die durch die schnelle Drehung der Platte entstehenden Luftwirbel, den Tonkopf im schwebenden Zustand belassen. Dadurch entsteht also kein direkter Kontakt zwischen Tonkopf und Magnetscheibe, sie wird somit auch nicht abgenutzt. Aus technischen Gründen fasst man meistens vier Scheiben übereinander angeordnet in einem Gehäuse zusammen. Da man zusätzlich, wie bei der Diskette, Ober- und Unterseite benutzt, benötigt man somit für eine derartige Anordnung 8 Magnetköpfe. Festplatten gestatten eine Speicherdichte, die weit über das 1.000-fache einer Diskette gehen kann. Im Gegensatz zu diesen sind sie jedoch erheblich teurer. Die größte Gefahr für Festplattenlaufwerke ist ein so genannter Head-Crash, d.h. der eigentlich schwebende Magnetkopf schlägt durch Erschütterung oder erhöhte Temperatur auf der Festplatte auf, wobei die äußerst empfindliche Magnetschicht und somit auch die Daten zerstört werden.

Festplattenlaufwerke werden auch als Harddisk (engl.) bezeichnet.
Eine Festplatte (Hard Disk Drive (HDD)) besteht aus einer oder mehreren starren Metallplatten, die mit besonders gutem magnetisierbaren Material beschichtet sind, das sehr hohe Schreibdichten erlaubt.

Dadurch können auf den einzelnen Platten erheblich mehr Spuren und Sektoren aufgezeichnet werden als auf Disketten, obwohl sie den gleichen Durchmesser haben. Eine Festplatte kann zum Beispiel 600 oder auch über 1.000 Spuren aufweisen.

Ausschlaggebend dafür ist die Kapazität und Bauart der Festplatte. Laufwerke für Personal-Computer verfügen je nach Spurdichte und Plattenanzahl über Speicherkapazitäten zwischen 1.600 und 12.000 MByte (1 Megabyte = 1.024 KByte = 1.048.576 Byte) und darüber. Auf einem 300 MByte Laufwerk ließe sich die komplette „Brockhaus Enzyklopädie" abspeichern.

Trotz der ungeheuren Speicherkapazität können die gespeicherten Daten zehn Mal so schnell gefunden werden wie bei einer Diskette. Ein Grund dafür ist die hohe Umdrehungsgeschwindigkeit der Platten, die bis zu 10.000 Umdrehungen pro Minute beträgt.

Gruppe	Bezeichnung	Kapazität
Magnetspeicher	Diskette	1,44 MB
	Zip - Diskette	100 MB
	Festplatte	bis 500 GB
	Wechselplatte	bis 500 GB
	Magnetband	(abhängig von der Länge) 80, 120, 250 bis 4.000 MB
	Magnetkarte	< 1 MB
Optische Speicher	CD-ROM	ca. 700 MB
	Digital Versatile Disc (DVD)	bis zu 17 GB
Flash-Speicher	USB-Stick	ca. 16 GB
	Speicherkarte (SD, MMC, …)	32 GB

4.1.4.1. Digital Versatile Disc (DVD)

Die DVD ist ein digitales Speichermedium, das einer CD ähnelt, aber über eine deutlich höhere Speicherkapazität (z. B. 4,7 GB) verfügt. Sie zählt zu den optischen Datenspeichern.

Das Backronym2 „DVD" ging auf die Abkürzung von Digital Video Disc und später Digital Versatile Disc (engl. für digitale vielseitige Scheibe) zurück, ist seit 1999 aber nach Angaben des DVD-Forums ein eigenständiger Begriff ohne Langform. In der Alltagssprache wird

der Ausdruck „DVD“ im Zusammenhang mit Filmen häufig im Sinne des logischen Formats DVD-Video verwendet.

4.1.4.2. Aufbau der DVD

Die DVD ist eine Weiterentwicklung der CD. Der Außendurchmesser beträgt 120 mm (in einem kleineren Format 80 mm), die Dicke 1,2 mm. Die DVD besteht aus zwei Halbdiscs mit einer jeweiligen Stärke von 0,6 mm. Außerdem ist es möglich, nur eine Halbdisc mit Daten zu beschreiben. Auf einer Halbdisc der DVD können sich eine oder zwei Informationsschichten (Layer) befinden.

Die DVD gibt es in zahlreichen Varianten, welche als DVD-Formate bezeichnet werden:

- Spezielle DVD-Formate, die für bestimmte Verwendungszwecke optimierte Datenstrukturen aufweisen und ursprünglich nur Lesezugriff erlaubten: DVD-Video, DVD-Audio, DVD-ROM und Hybrid-DVD.
- Für den Konsumenten beschreibbare DVD-Formate:
  - DVD-RAM, DVD-R, DVD+R, DVD-RW, DVD+RW, DVD-R DL, DVD+R DL

Besonders die einmal beschreibbaren Formate und die DVD-RAM lassen sich mit dem bloßen Auge von den gepressten anhand ihrer Rückseite unterscheiden, da diese aufgrund ihrer Legierungen Farben wie etwa blau, violett oder braun aufweisen. Die DVD-RAM hat außerdem charakteristisch sichtbare Sektormarken.

Format	Kapazität	Schichten Vorderseite/ Rückseite	Bemerkung
DVD-5	4,7GB (4,38GB/4483 MB)	1/0	
DVD-9	8,5GB (7,92GB/ 8110 MB)	2/0	Durch Neufokussieren des Lasers auf die zweite Schicht kann diese gelesen werden (*Dual-Layer-DVD*).
DVD-10	2 × 4,7GB	1/1	Zweiseitig beschrieben, muss gedreht werden (*Flipper*).
DVD-14	8,5GB + 4,7GB	2/1	Eine Seite *Dual Layer* (zwei Schichten) und eine *Single Layer* (eine Schicht).
DVD-18	2 × 8,5GB	2/2	Beide Seiten werden in zwei Schichten beschrieben. Selten.
DVD-Plus	4,7GB	1/1	DVD-5 wird mit einer normalen CD kombiniert. So kann der CD-Teil auf CD-Playern abgespielt werden. Die CD-Seite und die DVD-Seite sind

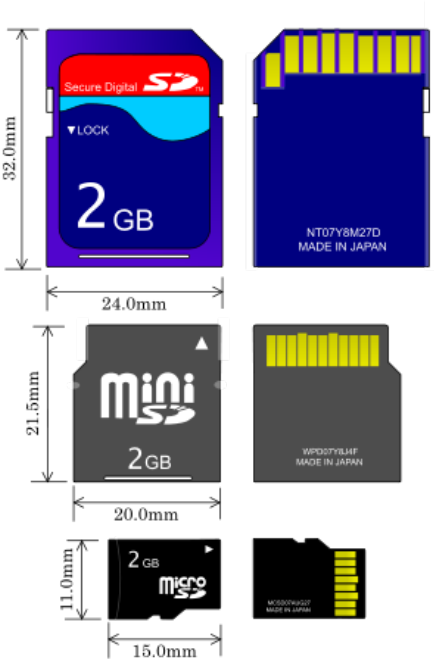
unterschiedlich, die Medien sind nicht normgerecht, sondern zu dick. Daher wird meist vom Abspielen solcher Medien in Laufwerken mit Einzugsschlitz, sogenannte Slot-In-Laufwerke, abgeraten. Wird von der Firma Sony unter dem Begriff *DualDisc* vermarktet.

Die zweite Informationsschicht wird aus Gründen der Datensicherheit nicht so dicht wie die erste beschrieben. Deshalb verdoppelt sich die Kapazität durch hinzufügen der zweiten Informationsschicht nicht ganz.

Die DVD wird wie die CD-ROM in einem spiralförmigen Track beschrieben. Der Abstand der Tracks beträgt bei der DVD 0,74 µm (CD: 1,6 µm).

4.1.4.3. Flash-Speicher

Flash-Speicher sind digitale Speicherchips; die genaue Bezeichnung lautet Flash-EEPROM. Im Gegensatz zu „gewöhnlichen" EEPROM-Speicher lassen sich beim Flash-EEPROM Bytes, die kleinsten adressierbaren Speichereinheiten, nicht einzeln löschen.



Der Name „Flash" kam durch eine Anekdote aus dem Entwicklungslabor von Toshiba 1984 zustande: Shoji Ariizumi, ein Mitarbeiter des Projektleiters Dr. Fujio Masuoka, erinnerte der blockweise Löschvorgang des Speichers an das blendende Licht eines Kamerablitzes. Er schlug deshalb den Namen „Flash" vor.

Anwendung finden Flash-Speicher überall dort, wo Informationen persistent (nichtflüchtig) auf kleinstem Raum – ohne permanente Versorgungsspannung – gespeichert werden müssen.

Häufige Verwendung finden sie in Form von USB-Speichersticks, verkürzt USB-Sticks genannt. Durch ihre höhere Speicherkapazität und Zugriffsgeschwindigkeit sowie ihre einfachere Handhabung haben sie andere Massenspeicher mit ähnlichem Anwendungsprofil wie die Diskette, die CD-RW und das Iomega Zip verdrängt.

Die ersten Sticks kamen im Jahr 2000 mit einer Speicherkapazität von 8 Megabyte auf den Markt. Mittlerweile gibt es Produkte mit einer

Kapazität von bis zu 256 Gigabyte mit 20 MB/s Lese- und 10 MB/s Schreibgeschwindigkeit (Stand: Juli 2009) – und auch wasserdichte Modelle.

Gelegentlich ist portable Software vorinstalliert, beispielsweise zur Datenverschlüsselung auf dem Stick. Die maximalen Datenraten für USB-Sticks liegen mittlerweile (Stand: 2010) bei 35 MB/s für das Lesen und 30 MB/s für das Schreiben. Die Abmessungen von USB Sticks werden immer geringer. Die kleinsten Sticks haben inkl. Schutzkappe eine Abmessung von lediglich 19,5mm x 15,5mm x 7mm (Stand: Juni 2010).

4.2. Software

Ohne Software funktionieren die einzelnen Bestandteile eines Computers nicht. Es gibt verschiedene Arten von Software. Einige bilden das Grundgerüst, andere dienen dem Komfort und wiederum andere dienen der Durchführung konkreter Aufgaben. Man kann dies mit dem Aufbau eines Gebäudes vergleichen. Als Fundament ist das Betriebssystem vorhanden. Ohne dieses funktioniert Ihre Hardware nicht.

Darauf kann weitere Software aufsetzen. Diese kümmert sich jetzt um bestimmte Aufgaben wie z. B. grafische Unterstützung, Texterstellung, Sammlung von Daten usw. Im Folgenden lernen Sie in der Verwaltung gängige Software kennen. Hierbei wird der Oberbegriff erläutert. Der Umgang mit konkreten Programmen dieser Software ist Bestandteil der Präsenzphase.

Standardsoftware individuelle Anpassungen				**Individualprogramme**	
Textverarbeitung	Tabellenkalkulation	Datenbanken	Grafik	Programmiersprachen	Spezialprogramme (TOOLS)
Benutzeroberfläche (z. B. Windows)					
Betriebssystem					

4.2.1. Betriebssystem

Ein Betriebssystem – wozu?

Die Hardware eines Computersystems allein ist nicht funktionsfähig. Ihre Möglichkeiten sind nach der Durchführung des Selbsttests erschöpft. Dieser Selbsttest ist ein kleines Programm, mit dem die Konfiguration erkannt und ihre Funktionsfähigkeit getestet wird. Das Programm ist in den beiden fest im System eingebauten ROM-Chips hin-

terlegt und läuft beim Einschalten automatisch ab. Dieses Programm, also eine Software, ist durch die ROM-Chips fest im Computer eingebaut. Eine solche Software in ROM-Chips, also Software in Form von Hardware, nennt man Firmware.

Jedes Computersystem benötigt für alle über den Selbsttest hinausgehenden Funktionen eine Software, die einen gewissen Grundbestand an Verarbeitungsrichtlinien, eine Sammlung von kleinen Programmen, von Standardfunktionen (Routinen) zur Verfügung stellt. Eine solche Sammlung von kleinen Programmen nennt man Betriebssystem. Das Betriebssystem ermöglicht z. B. das Schreiben von Informationen auf den Bildschirm, das Ansprechen von Druckern oder das Lesen einer Tastatureingabe. Betriebssysteme sind meist sehr stark auf die Hardware, hier insbesondere auf die Möglichkeiten des verwendeten Prozessors zugeschnitten. Meist sind Betriebssysteme auch für eine ganz bestimmte Art der Nutzung konzipiert; z. B. dafür, ob nur ein Anwender oder aber mehrere Anwender zur gleichen Zeit mit dem System arbeiten sollen. Oder dafür, dass eine oder mehrere Anwendungen (Programme) zur gleichen Zeit ablaufen können.

Die vom Betriebssystem zur Verfügung gestellten Grundfunktionen werden vom Benutzer direkt genutzt. Auch alle Programme nutzen mittelbar die von dem Betriebssystem zur Verfügung gestellten Routinen, z. B. die Standardprogramme Textverarbeitung, Grafik, Tabellenkalkulation oder Datenbank. Sie alle nutzen die Routinen des Betriebssystems um Daten auf den Bildschirm zu schreiben, auf Datenträger zu speichern oder von diesen zu lesen.

Die Betriebssysteme fallen zusammen mit den Dienstprogrammen, den Programmiersprachen (incl. Compiler[2] / Interpreter[3]), der Netz- und Datenfernübertragungs-(DFÜ) Software u.a. in den Bereich der Systemsoftware.

Ein Betriebssystem ist die Software, die die Verwendung (den Betrieb) eines Computers ermöglicht. Es verwaltet Betriebsmittel wie Speicher, Ein- und Ausgabegeräte und steuert die Ausführung von Programmen.

Betriebssystem heißt auf Englisch operating system (OS). Dieser englische Ausdruck kennzeichnet den Sinn und Zweck: Die in den Anfängen der Computer stark mit schematischen und fehlerträchtigen Arbeiten beschäftigten Operatoren schrieben Programme, um sich die Arbeit zu erleichtern; diese wurden nach und nach zum operating system zusammengefasst.

Betriebssysteme bestehen in der Regel aus einem Kern (englisch: Kernel), der die Hardware des Computers verwaltet, sowie grundlegenden Systemprogrammen, die dem Start des Betriebssystems und dessen Konfiguration dienen. Unterschieden werden Einbenutzer-

[2] Übersetzungsprogramm, das ein Primärprogramm in einem mehrstufigen Prozess in ein Objektprogramm umwandelt, das dann beliebig oft benutzt werden kann.

[3] Übersetzungsprogramm, hat einen Aufbau, durch den es jeden Befehl oder jede Anweisung des Primärprogramms sofort übersetzt und ausführt. Es entsteht dabei aber kein Objektprogramm.

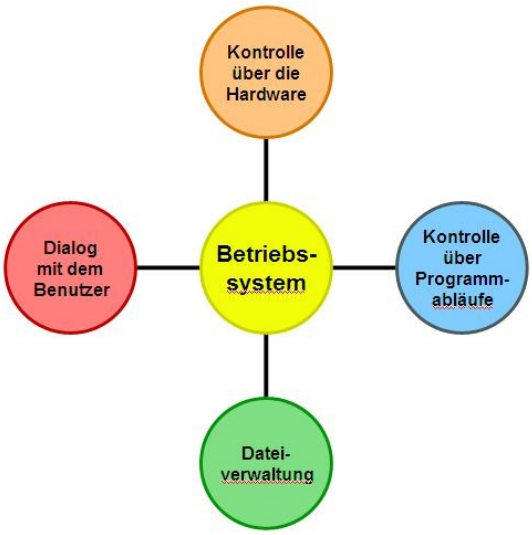
und Mehrbenutzersysteme, Einzelprogramm- und Mehrprogrammsysteme, Stapelverarbeitungs- und Dialogsysteme. Betriebssysteme finden sich in fast allen Computern: als Echtzeitbetriebssysteme auf Prozessrechnern, auf normalen PCs und als Mehrprozessorsysteme auf Hosts und Großrechnern.

4.2.1.1. Hauptaufgaben eines Betriebssystems

Ein Betriebssystem ist in der Regel das Hauptsteuerprogramm, das alle anderen System- und Arbeitsprogramme (System- oder Anwendersoftware) steuert oder überwacht.

Job-Management	Ermöglicht das Abarbeiten von Befehlen
Data-Management	Realisiert den Zugriff auf das Speichern von Daten
User-Management	Stellt die Benutzerschnittstelle zwischen dem Anwender und der Maschine dar, das heißt die Anweisungen des Anwenders werden in einen für den Rechner verständlichen Code umgewandelt.

4.2.1.2. Aufgaben eines Betriebssystems



- überprüft die Leitungen zu Bildschirm, Tastatur, Drucker etc.
- sucht Informationen (Daten) auf externen Speichern
- sucht freien Speicherplatz auf externen/internen Speichern
- wandelt die Anweisungen an den Rechner in einen für ihn verständlichen Code um
- steuert den Ablauf der verschiedenen Programme
- überwacht die Zusammenarbeit der einzelnen Systemkomponenten und Peripheriegeräte
- unterstützt bei der Programmentwicklung

Kontrolle über die Hardware

Im Betriebssystem ist die Existenz und Art der angeschlossenen Peripheriegeräte mittels so genannter Gerätetreiber bekannt. Das Betriebssystem koordiniert die Zusammenarbeit des Computers mit den Peripheriegeräten.

Kontrolle über den Programmablauf
Die Anwenderprogramme haben nicht die Möglichkeit selbst die Hardware zu steuern, sondern geben ihre Befehle an das Betriebssystem weiter.

Dateiverwaltung

Ähnlich dem Verwalter eines großen Lagers ist das Betriebssystem in der Lage, den Speicherplatz jedes externen Datenträgers so zu verwalten, dass es jederzeit die noch freien Plätze auf dem Datenträger sowie die Position jeder einzelnen darauf gespeicherten Datei kennt. Dieser Umstand erlaubt einen direkten Zugriff auf eine Datei, ohne nach ihr zu suchen.

Dialog mit dem Benutzer

Zum Betriebssystem gehört auch der so genannte Kommandointerpreter. Der Interpreter ist zum Dialog mit dem Benutzer bereit, sobald der Prompt (Bereitschaftszeichen) erscheint. Die häufigste Form ist ”C:\>”. Zu zwei Dingen kann dann der Kommandointerpreter genutzt werden:

Programmaufruf

Der Programmname oder eine Abkürzung davon werden hinter dem Prompt-Zeichen eingegeben. Danach wird die Taste „Return” gedrückt. Bei grafischen Benutzeroberflächen wird in der Regel ein Programmsymbol mit Hilfe der Maus durch anklicken gestartet.

Eingabe von Betriebssystemkommandos

Befehle an das Betriebssystem können in einer bestimmten Kommandosprache eingegeben werden. Um mit dem Kommandointerpreter des Betriebssystems zu arbeiten, muss dessen Kommandosprache erlernt werden.

4.2.1.3. Graphische Benutzeroberfläche

Eine Benutzeroberfläche entspricht dem Bild, das sich Ihnen bietet, wenn Sie den Rechner gestartet und das Betriebssystem geladen haben.

Eine grafische Benutzeroberfläche versucht den Anwender dahingehend zu entlasten, dass er sich keine einzelnen Befehle mehr merken muss. Anstelle der Befehle treten bunte Bildchen (so genannte Icons), die eine bestimmte Funktion veranschaulichen. Klickt der Benutzer mit der Maus auf eines dieser Bildchen, wird die zugrunde liegende Funktion ausgeführt. Dies kann z. B. das Drucken oder Speichern eines Textes sein.

4.2.1.4. Kommandoorientiertes Betriebssystem

Bei einem kommandoorientierten Betriebssystem sieht dieses sehr einfach aus. Die Befehle müssen Sie über die Tastatur eingeben. Da sie eine Art Fremdsprache darstellen, benötigen Sie einige Zeit und Übung bis ein zufrieden stellendes Arbeiten möglich ist.

4.3. Anwendungssoftware

Ein Anwendungsprogramm (kurz „Anwendung“) ist ein Computerprogramm, das eine für den Anwender nützliche Funktion ausführt, z. B. Buchhaltung, Informationssysteme, Computer Aided Design (CAD), Textverarbeitung, Tabellenkalkulation oder auch Spiele. Aus dem englischen Begriff Application hat sich in der Alltagssprache auch die Bezeichnung „Applikation“ für Anwendungsprogramm eingebürgert.

Anwendungsprogramme werden in erheblichem Umfang zur Unterstützung der Verwaltung in Behörden und Unternehmen eingesetzt. Anwendungssoftware ist nur zum Teil Standardsoftware. Zu einem großen Teil werden auf den jeweiligen Anwendungsfall zugeschnittene Branchenlösungen oder Individuallösungen eingesetzt.

Als Standardsoftware werden Softwaresysteme verstanden, die einen klar definierten Anwendungsbereich abdecken und als vorgefertigte Produkte erworben werden können. Im Gegensatz dazu wird Individualsoftware gezielt für den Einsatz bei einem Kunden bzw. Unternehmen entwickelt. Gelegentlich wird noch zwischen Standardanwendungssoftware und Standardsystemsoftware unterschieden. Im Bereich der Systemsoftware ist allerdings der Einsatz von Standardsoftware nahezu selbstverständlich, so dass dieser Begriff kaum verwendet und auf diese Unterscheidung meist verzichtet wird.

Funktionsbezogene oder funktionsübergreifende Standardsoftware ist branchenneutral und auf einen bestimmten Einsatzbereich zugeschnitten, der in vielen Fällen stark geregelt ist, beispielsweise durch gesetzliche Vorgaben. Der Übergang zwischen funktionsbezogener und -übergreifender Software ist fließend, typische Beispiele für funktionsbezogene Standardsoftware sind Office-Pakete, Buchhaltungssoftware oder CAD.

Office-Pakete sind Zusammenstellungen gebräuchlicher Software für Arbeiten im Büro, welche unterschiedliche dort anfallende Aufgaben erledigen oder zumindest unterstützen sollen. Dazu gehören in den meisten Fällen Textverarbeitungs-, Tabellenkalkulations-, Präsentations- und Datenbank-Programme.

4.3.1. Textverarbeitung

Eine Textverarbeitungssoftware ist heutzutage die am häufigsten eingesetzte Standardsoftware in der Verwaltung. Fast überall fällt Schriftverkehr an und bei einer vorhandenen Ausstattung mit PC wird meist auch gleich eine Textverarbeitungssoftware bereitgestellt. Neben den herkömmlichen Funktionen einer Schreibmaschine, bietet die Textverarbeitung eine Vielzahl von weiteren Funktionen an. Diese werden hier aufgeführt. Um ein besseres Verständnis zu erzielen, werden diese im Präsenzunterricht näher erläutert.

In der Berliner Verwaltung hat sich Microsoft WORD als Standardtextverarbeitung etabliert.

4.3.1.1. Funktionen zur Unterstützung der Texteingabe

- Sofortkorrektur
- Positionsanzeige (Seite, Zeile und Spalte)
- horizontales und vertikales Blättern im Text
- automatischer Zeilenumbruch und Seitenumbruch - Tabulatoren
- Speicher für Textbausteine - Silbentrennung
- Überprüfung auf Rechtschreibfehler

4.3.1.2. Funktionen zur Verbesserung des Schriftbildes

- Absatzformate wie z. B. Blocksatz (d.h. Text ist links- und rechtsbündig. Im Text sind die Leerzeichen notfalls breiter), Zentrieren sowie rechts- und linksbündiger Flattersatz
- WYSIWYG (What you see is what you get), d.h. das Bild auf dem Bildschirm entspricht dem, was ausgedruckt wird.
- Zeichenformate wie z. B. Unterstreichen, Fettdruck, Kursivschrift, unterschiedlicher Zeilenabstand, unterschiedliche Schriftbreite (10, 12 oder 15 Zeichen pro Zoll sowie Proportionalschrift), unterschiedliche Schrifttypen und Schriftgrößen.
- Sonderzeichen und Umrandungen
- Einbinden von Grafik

4.3.2. Textmengenorientierte Funktionen

- Ersetzen, Umstellen, Kopieren und Löschen von Textmengen (einzelne Zeichen, Wörter, Sätze oder Absätze)
- Suchen von Begriffen in einem Text
- Suchen und Ersetzen
- Bausteinkorrespondenz
- Erstellen von Serienbriefen

4.3.2.1. Textbaustein

Bestimmte Textstellen können markiert und kopiert oder gelöscht und anschließend an anderen Stellen des Textes eingefügt werden. Häufig wiederkehrende Textstellen können auch als Textbaustein in einer eigenen Datei gespeichert und in andere Texte eingefügt werden. So ist es möglich, einen Brief fast nur aus Textbausteinen zusammenzusetzen, zum Beispiel für Briefkopf, Anrede, den eigentlichen Inhalt und den Briefschluss.

4.3.2.2. Autokorrektur

Eingebaute Funktion die nach bestimmten Begriffen sucht, die automatisch durch andere Begriffe ersetzt werden.

4.3.2.3. Serienbrief

Ein Serienbrief ist ein Dokument, das an viele Empfänger versendet wird. Adresse, Anrede und Teile des Inhalts sind meist personalisiert und können den Anschein eines persönlichen Anschreibens erwekken.

In der Regel werden Serienbriefe computerbasiert erstellt. Grundlage ist eine Datenquelle und eine Vorlage.

Die Datenquelle enthält die variablen Daten (z. B. Name, Anschrift, Anrede), die in die Vorlage integriert werden. Zusätzlich können mit den Informationen der Datenquelle zielgruppengerechte Serienbriefe erstellt werden. Zum einen können die Adressen nach verschiedenen Kriterien gefiltert werden, um nur eine bestimmte Zielgruppe anzuschreiben. Zum anderen können Teile des Inhalts an Bedingungen geknüpft werden, um eine weitere Individualisierung zu erreichen.

Die Erstellung von Serienbriefen wird von den meisten Textprogrammen unterstützt. Die Abwicklung von Serienbriefen wird teilweise von externen Dienstleistern durchgeführt. Sie können neben Datenpflege, Druck und Kuvertierung auch die Portooptimierung übernehmen. Damit werden bei großen Stückzahlen personelle und finanzielle Ressourcen des Versenders geschont.

Die Erstellung eines Serienbriefes wird im Anhang 5 näher erläutert.

4.3.3. Dokumentbezogene Funktionen

- automatische Seitennummerierung
- automatische Erstellung von Kopf- und Fußzeilen
- automatische Erzeugung eines Inhaltsverzeichnisses
- automatische Nummerierung von Überschriften, Fußnoten und Abbildungen
- Fußnotenbehandlung
- Behandlung von Vorwort und Anhang

4.3.3.1. Speicherungs- und Wiedergabefunktionen

- Archivieren
- Löschen, Kopieren und Umbenennen von Dokumenten, Textrecherche (Suche von Textteilen) über mehrere Dokumente
- gleichzeitiges Drucken und Erfassen von Texten (Drucken im Hintergrund)

4.3.3.2. Programmierbarkeit

Vom Benutzer definierbare Kommandos oder Funktionstasten für häufig vorkommende Befehlsfolgen.

Rechenoperationen innerhalb von Textverarbeitungsdokumenten können in Makros gespeichert werden. Diese Makros können an

Schaltflächen gekoppelt werden und in der Menü- bzw. Symbolleiste abgelegt werden.

An dieser Zusammenfassung können Sie erkennen, dass moderne Textverarbeitungssysteme über eine Vielzahl von Funktionen verfügen, um die Erstellung von Briefen und langen Texten wie Büchern zu erleichtern. Nicht alle Programme haben diese Möglichkeiten.

4.3.4. Tabellenkalkulation

Der Begriff Tabellenkalkulation bezeichnet eine Gruppe von Computerprogrammen, die für unterschiedlichste rechnerische Aufgaben eingesetzt werden. Sie können mit ihnen alle Berechnungen durchführen, für die Sie sonst einen Taschenrechner benötigen. Allerdings haben Sie bei der Benutzung von Kalkulationsprogrammen den Vorteil einer großen Zeitersparnis bei wiederkehrenden Aufgaben.

Stellen Sie sich folgende Aufgabe vor: Sie wollen laufend die aktuellen Ausgaben Ihres Haushaltes berechnen. Der Kostenrahmen ist streng geplant, doch andauernd kommen neue Ausgaben und unvorhergesehene Entwicklungen dazu. Mit Papier, Bleistift und Taschenrechner ist dies eine mühevolle Arbeit.

Ein Tabellenkalkulationsprogramm befreit Sie von der von Fehlern anfälligen und sich wiederholenden Arbeit, Beträge zu errechnen. Der Grundgedanke bei diesen Programmen ist, dass sehr oft tabellenartige Zahlenaufstellungen bearbeitet werden.

Statt eines Blattes Papier verwenden Tabellenkalkulationsprogramme eine Tabelle, das sogenannte Arbeitsblatt. Nur ein Ausschnitt dieser Tabelle ist auf dem Bildschirm sichtbar. Dieses Arbeitsblatt ist horizontal und vertikal in Zeilen bzw. Spalten unterteilt.

Sie können sich das wie bei dem Spiel „Schiffe versenken“ vorstellen. Die Schnittstellen ergeben Felder, in die Zahlenwerte, Rechenanweisungen an den Computer oder erklärender Text eingegeben und in denen die Ergebnisse angezeigt werden.

Besonders viel Komfort wird demjenigen geboten, der oft ähnliche Berechnungen durchzuführen hat. Das Basismodell der Berechnung kann jederzeit neu benutzt werden.

Besondere Einsatzgebiete von Tabellenkalkulationsprogrammen sind u.a.:

- Finanzmathematische Berechnungen
- Statistische Funktionen
- Umsetzung der Ergebnisse in Grafiken
- In der Berliner Verwaltung hat sich Microsoft EXCEL als Standardtabellenkalkulation etabliert.

4.3.5. Datenbank

Eine Datenbank ist eine abgeschlossene Einheit, in der große Mengen von Informationen (Daten) gesammelt werden. Dabei erfolgt eine Auswahl der Informationen nach bestimmten Kriterien und die Daten werden geordnet, so dass ein möglichst schnelles Auffinden möglich wird.

Der Unterschied zu einer Text- oder Tabellenkalkulationsdatei besteht darin, dass hier zwar auch Daten enthalten, diese jedoch ungeordnet sind und daher nicht in der gleichen Geschwindigkeit sortiert und gefiltert werden können.

Ein weiterer Unterschied liegt darin, dass man in einer Datenbank mehrere Tabellen ablegen kann, die miteinander verknüpft werden können.

Beispiele für Datenbanken sind:

- Adressbücher
- Verkehrssünderdatei in Flensburg
- Patientendatenbanken in Krankenhäusern
- Personalverwaltungen
- Schufa
- Flugbuchungssysteme
- Lagerbestände, -haltung
- DB zum Schreiben von Rechnungen, Buchhaltung
- OPEN/Prosoz
- POLIKS
- Musika
- IPV
- KiTA

Die Eigenschaften einer Datenbank lauten:

- Schnelligkeit beim Auffinden der Informationen
- Vollständigkeit der Informationen
- Zugänglichkeit an verschiedenen Orten
- zentrale Datenspeicherung
- vielfältige Fragestellungen sind möglich

Es gibt verschiedene Strukturen von Datenbanken und Daten:

4.3.5.1. Volltextdatenbanken

Es werden gesamte Texte gespeichert, z. B. die Zeitung ”Handelsblatt”, es können ganze Artikel abgerufen werden. Wären diese Texte ohne Ordnung und Systematisierung gespeichert, müsste der Rechner bei einer Anfrage erst sämtliche Texte durchlesen, um den richtigen Artikel aufzufinden. Es sind also Zusatzinformationen notwendig, um den Suchvorgang zu beschleunigen.

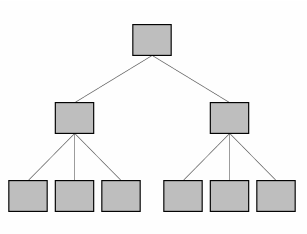
Hierfür gibt es sog. Indices, also Schlagwortregister. Dieser Index ist alphabetisch sortiert und macht das gezielte Suchen von Artikeln, Textpassagen oder nur bestimmten Stichworten möglich. Beim Einlesen der Artikel werden alle wichtigen Schlagwörter in einen Grundindex aufgenommen.

4.3.5.2. Bibliografische Datenbanken

Bibliografische Datenbanken sind Literaturdatenbanken zu einem bestimmten Fachgebiet oder Thema und enthalten bibliografische Angaben wie Verfasser, Titel und Erscheinungsjahr eines Werkes, manchmal auch eine kurze Annotation.

4.3.5.3. Hierarchische Datenbanken

Ein hierarchisches Datenbankmodell ist das älteste Datenbankmodell, es bildet die reale Welt durch eine hierarchische Baumstruktur ab. Jeder Satz (Record) hat also genau einen Vorgänger, mit Ausnahme genau eines Satzes, nämlich der Wurzel der so entstehenden Baumstruktur.



Die Daten werden in einer Reihe von Datensätzen gespeichert, mit denen verschiedene Felder verknüpft sind. Die Instanzen eines bestimmten Datensatzes werden als Datensatzabbild zusammengefasst. Diese Datensatzabbilder sind vergleichbar mit den Tabellen einer relationalen Datenbank.

4.3.5.4. Relationale Datenbanken

Eine relationale Datenbank dient zur elektronischen Datenverwaltung in Computersystemen und beruht auf dem relationalen Datenbankmodell. Dieses wurde 1970 von Edgar F. Codd erstmals vorgeschlagen und ist bis heute, trotz einiger Kritikpunkte, ein etablierter Standard für Datenbanken.

Das zugehörige Datenbankmanagementsystem wird als relationales Datenbankmanagementsystem oder RDBMS bezeichnet. Zum Abfragen und Manipulieren der Daten wird überwiegend die Datenbanksprache SQL (Structured Query Language) eingesetzt, die ebenfalls von Codd entwickelt wurde.

Grundlage des Konzeptes relationaler Datenbanken ist die Relation, ein im mathematischen Sinn wohldefinierter Begriff. Sie stellt eine mathematische Beschreibung einer Tabelle dar; siehe Datenbankrelation.

Hier werden die verschiedenen Daten in verschiedenen Tabellen gespeichert, die Daten können zueinander in Relationen, also ins Verhältnis gesetzt werden.

Es gibt z. B. eine Tabelle in der alle Lieferanten stehen und eine Tabelle in der alle Möbel aufgeführt werden.

Tabelle der Lieferanten

a	Lieferant 1
b	Lieferant 2
c	Lieferant 3

Tabelle der Möbel

a	Schrank 1
b	Stuhl
c	Tisch
d	Schrank 2
e	Couch
f	Sessel

Die Vorteile eines relationalen Datenbanksystems:

- Alle Dateien sind nur in jeweils einer Tabelle gespeichert. Es werden keine Daten doppelt eingegeben, dadurch werden auch Fehler vermieden.
- Datenänderungen fallen leichter, da die Änderungen nur noch in einer Tabelle notwendig sind.
- Die Relationen werden bei Neueinträgen, automatisch angelegt.
- Der benötigte Speicherplatz wird auf ein Minimum reduziert.

Microsoft Access ist, wie die meisten Datenbanksprachen, eine relationale Datenbank und wird in der Berliner Verwaltung verwendet.

4.3.5.5. Bestandteile einer Datenbank

In einer Datenbank werden in der Regel eine unbestimmte Anzahl von Datensätzen gespeichert.

Ein Datensatz ist eine abgeschlossene Einheit innerhalb einer Datenbank. Er enthält typischerweise mehrere Datenfelder, die sich in der Struktur und Beschaffenheit in jedem weiteren Datensatz derselben Datei oder Datenbank wiederholen.

Wird die Datenbank als Tabelle dargestellt, so entspricht ein Datensatz einer Tabellenzeile. In einer Kartei entspricht ein Datensatz einer einzelnen Karteikarte. Oft wird ein Datensatz wegen der besseren Übersicht als Formular auf einer Seite dargestellt, ähnlich einer großen Karteikarte.

Dem Datenfeld können verschiedene Eigenschaften wie Größe, Format usw., zugewiesen werden.

4.4. Open Source Software

Open source (engl.) bzw. quelloffen ist Software, die unter einer von der Open Source Initiative (OSI) anerkannten Lizenz steht. Die OSI stützt sich bei der Bewertung auf die Kriterien der Open Source Definition, die weit über die Verfügbarkeit des Quelltexts hinausgeht

und fast deckungsgleich mit sog. Freier Software ist, d. h. der Quelltext muss auch offen für Bearbeitung und Weiterverbreitung sein.
Die Open Source Initiative wendet den Begriff Open Source auf all die Software an, deren Lizenzverträge den folgenden drei charakteristischen Merkmalen entsprechen:

- Die Software (d. h. der Quelltext) liegt in einer für den Menschen lesbaren und verständlichen Form vor: In der Regel handelt es sich bei dieser Form um die Quelltexte in einer höheren Programmiersprache. Vor dem eigentlichen Programm(ab)lauf ist es normalerweise notwendig, diesen Text durch einen so genannten Compiler in eine binäre Form zu bringen, damit das Computerprogramm vom Rechner ausgeführt werden kann. Binärprogramme sind für den Menschen im semantischen Sinne praktisch nicht lesbar.

- Die Software darf beliebig kopiert, verbreitet und genutzt werden: Für Open-Source-Software gibt es keine Nutzungsbeschränkungen. Weder bezüglich der Anzahl der Benutzer, noch bezüglich der Anzahl der Installationen. Mit der Vervielfältigung und der Verbreitung von Open-Source-Software sind auch keine Zahlungsverpflichtungen gegen einen Lizenzgeber verbunden.

- Die Software darf verändert und in der veränderten Form weitergegeben werden: Durch den offengelegten Quelltext ist Verändern ohne weiteren Aufwand für jeden möglich. Weitergabe der Software soll ohne Lizenzgebühren möglich sein. Open-Source-Software ist auf die aktive Beteiligung der Anwender an der Entwicklung geradezu angewiesen. So bietet sich Open-Source-Software zum Lernen, Mitmachen und Verbessern an.

4.4.1. Beispiele für Open Source-Software

- Linux (Betriebssystem)
- OpenOffice (Anwendersoftware)

Im Bezirksamt Tempelhof-Schöneberg läuft ein Projekt zum Einsatz von OpenSource Software in der Berliner Verwaltung.

Es wurden Anforderungen an eine künftige IT-Landschaft erfasst und verschiedene Szenarien einer Realisierung beschrieben und miteinander verglichen.

Als kostengünstigtes Szenario hat sich ein möglichst grossflächiger Einsatz von Open Source erwiesen. Damit können Lizenz- und Hardwarekosten in Grössenordnungen gespart werden.

Innerhalb des Projekts wird die Realisierbarkeit von Pilotinstallationen getestet. An dieser Pilotierung sind Mitarbeiter aus mehreren Bezirksämtern beteiligt.

Um den laufenden Betrieb nicht zu stören, werden die Arbeiten in einem Labor mit abgeschottetem Netz durchgeführt.
Teilprojekte:

1. OES (eDirectory, File- und Printservices)
2. Linux Terminal Server
3. Linux (Thin- , Smart- und Fat Client)
4. Fachverfahren
5. ZENWorks
6. Office
7. Windows Terminal Server
8. Groupware

Da die meisten vorhandenen Fachverfahren weiter verfügbar sein müssen, musste diesem Aspekt besondere Aufmerksamkeit gewidmet werden.

4.5. Benutzeroberfläche

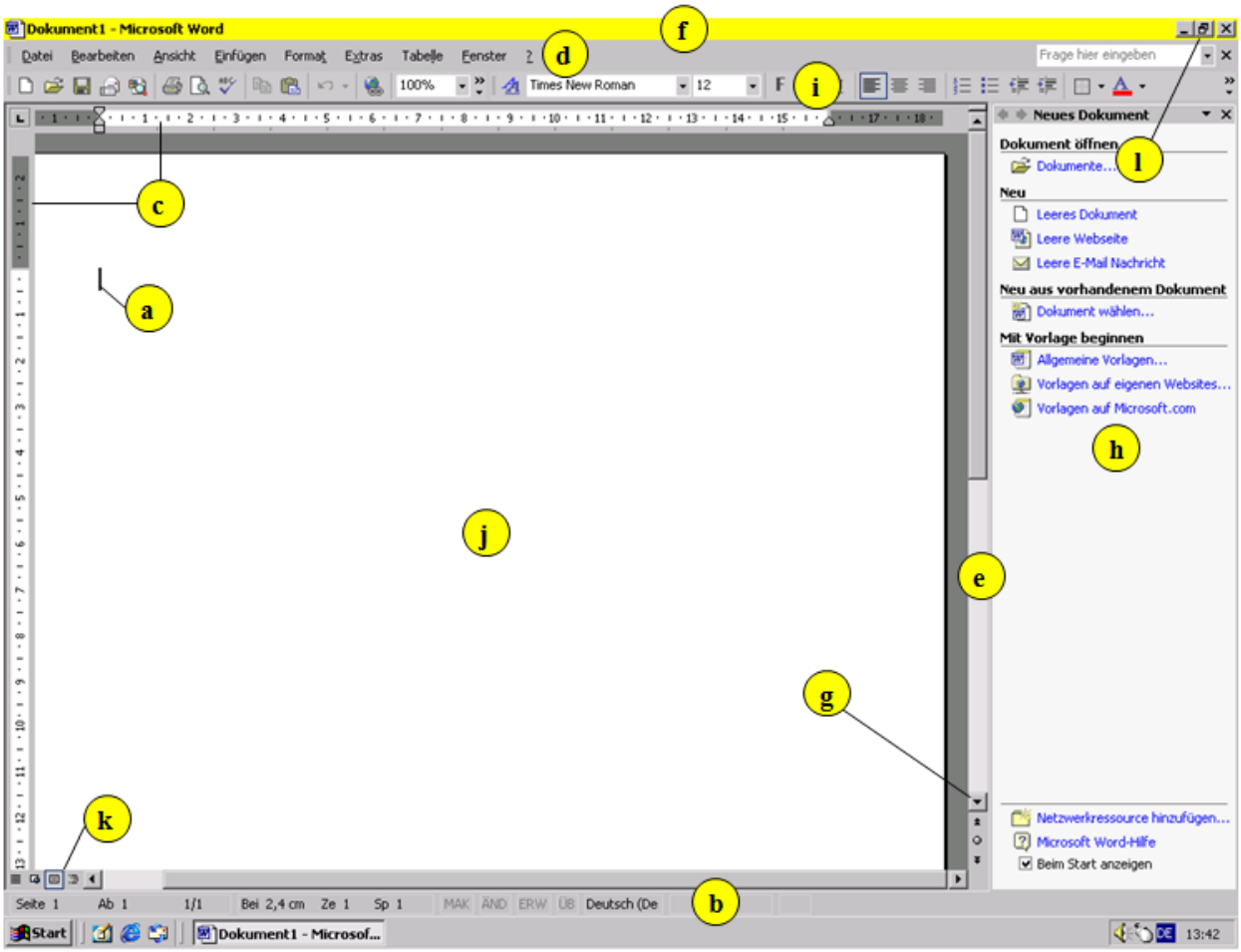
Die in der Berliner Verwaltung verwendete Standardsoftware umfasst in aller Regel die Produkte:

Microsoft WORD	→	**Textverarbeitung**
Microsoft EXCEL	→	Tabellenkalkulation
Microsoft ACCESS	→	Datenbank
Microsoft POWERPOINT	→	Präsentation
Microsoft OUTLOOK	→	Kommunikation

Alle Produkte haben eine nahezu einheitliche Benutzeroberfläche, die dem Anwender die Orientierung am Bildschirm erleichtert. Durch die einheitliche Gestaltung der Symbole für gleiche Befehle wird die Verwendung dieser Anwendungsprogramme auch für ungeübte Anwender simpel.

Insgesamt erreichen die Hersteller einen hohen Grad der Wiedererkennung.

Im Folgenden sollen die einzelnen Elemente der Benutzeroberfläche verdeutlicht werden:



a	Cursor	d	Menüzeile	g	Bildlaufpfeil	j	Arbeitsbereich
b	Statuszeile	e	Bildlauffeld	h	Aufgaben-bereich	k	Ansichten-steuerung
c	Lineale	f	Titelzeile	i	Symbolzeile	l	Mini-/Maximier-en, Schließen

Fragen zur Selbstkontrolle:

10. Was ist unter dem Begriff Hardware zu verstehen?
11. Aus welchen grundlegenden Bestandteilen besteht ein Computer?
12. Nennen Sie (mindestens) fünf Eingabegeräte!
13. Aus welchen zwei Hauptteilen besteht die Zentraleinheit?
14. Was ist unter dem Begriff RAM zu verstehen?
15. Welche externen Speicher gibt es?
16. Was sind Dateien?
17. Warum ist für den Betrieb eines Computers ein Betriebssystem notwendig?
18. Welche Hauptaufgaben hat ein Betriebssystem zu erledigen?
19. Was ist unter dem Begriff MS-Windows zu verstehen?
20. Nennen Sie für eine Textverarbeitung je zwei Funktionen zur Unterstützung der Texteingabe, zur Verbesserung des Schriftbildes und textmengenorientierte Funktionen!
21. Wofür werden Tabellenkalkulationsprogramme eingesetzt?
22. Was ist eine Datenbank?
23. Nennen Sie vier Ihnen bekannte Datenbanken!
24. Nennen Sie die Elemente der Benutzeroberfläche.

5. Netze und Postdienste

Lernziele:

Der/Die Lernende soll:

- erklären können, was ein Computer-Netzwerk ist,
- wissen, welche Vorteile und Gründe es für den Einsatz eines Computer-Netzwerkes gibt,
- die Begriffe für Netzwerkgrößen und Strukturen kennen,
- erklären können, was unter dem Begriff „Internet“ zu verstehen ist,
- erklären können, was die Unterschiede zwischen dem „Internet“ und dem „Intranet“ sind.

5.1. PC-Netzwerke

Durch den Einsatz von einem Standardbetriebssystem für PC hat man die Voraussetzung dafür geschaffen, dass jeder PC völlig unabhängig und eigenständig die anfallenden Arbeiten mit der vor Ort vorhandenen Hard-/Software und Daten erledigen konnte.

Die Idee, mehrere PC miteinander zu verbinden, basierte auf dem Wunsch, eine Vereinfachung des Datenaustausches und eine bessere Auslastung der Peripherie insbesondere bei Druckern und Massenspeichern zu erreichen. Außerdem soll der Ausschluss von Fehlerquellen wie z. B. bei der Parallelführung von zwei gleichen Dateien auf verschiedenen Rechnern (Redundanz) und die gleichzeitige Verfügbarkeit des aktuellen Datenbestandes für mehrere Nutzer erreicht werden.

Die Koppelung von PC in der beschriebenen Weise wird durch ein Netzwerk realisiert, wobei jedem einzelnen der angeschlossenen Rechner die normalen Funktionen weiterhin voll erhalten bleiben.

Unter einem PC-Netzwerk versteht man ein Verbundsystem zwischen mehreren Rechnern und Peripheriegeräten (Drucker, Plotter, Massenspeicher usw.). Das PC-Netzwerk ermöglicht einerseits unabhängiges Arbeiten auf jedem einzelnen angeschlossenen Rechner und andererseits gleichzeitigen Zugriff auf gemeinsame Einrichtungen.

Im Gegensatz zu einem Mehrplatzsystem unter einem mehrplatzfähigen Betriebssystem wie z. B. UNIX ist es in einem Personal-Computer-Netzwerk erforderlich, dass in allen angeschlossenen Rechnern ein eigener Prozessor und ein eigener Hauptspeicher vorhanden sind.

Dies gilt auch für so genannte Diskless / Medialess Workstations. Das sind PC mit eigenem Prozessor und Hauptspeicher aber ohne Speicherperipherie wie Festplatte oder Diskettenlaufwerk.

5.1.1. Technische Komponenten

Ein PC-Netzwerk benötigt in der Regel folgende Komponenten:

- PC für die einzelnen Arbeitsplätze
- PC für die zentrale Arbeitsabwicklung und Datenhaltung (File-Server)
- Netzwerkkarten
- Verbindungskabel, Verteiler
- Netzwerk-Betriebssystem
- Standard- und/oder Anwendersoftware

Während Software, Arbeitsstationen (Workstation) und File-Server unabhängig vom Netzwerk beschafft und auch eingesetzt werden können, gehören Netzwerkkarten, Verbindungskabel und Netzwerk-Betriebssystem direkt zum Netzwerk; sie sind ohne Netzwerkbetrieb nicht benutzbar.

5.1.2. Vorteile eines PC-Netzwerkes (Rechnerverbundsystem)

Ein Rechnerverbundsystem bietet eine Reihe von Vorteilen:

- *Kommunikationsverbund*
  Ein Benutzer kann mit allen anderen Benutzern der verbundenen Rechner Mitteilungen austauschen (elektronische Post).

- *Datenverbund*
  Jeder Datenbestand kann unabhängig vom Ort seiner Speicherung im Netz einem Benutzer zugänglich gemacht werden. Die Daten können zentral gespeichert werden und liegen für alle Teilnehmer immer in der aktuellsten Version vor.

- *Sicherheitsverbund*
  Die Daten können zwischen den Rechnern gegenseitig gesichert werden. Datensicherung kann zentral dort erfolgen, wo die Daten gespeichert sind.

- *Funktionsverbund*
  Ein Benutzer kann Programm- und Gerätefunktionen anderer Rechner des Netzwerks verwenden. Beispiel: Drucker oder Laufwerke.

- *Lastverbund*
  Aufträge werden je nach Auslastung des Rechners auf die verbundenen Rechner verteilt, um eine optimale Kapazitätsauslastung des Verbunds zu erreichen.

5.1.3. Netzwerkbetriebssystem

Das Netzwerkbetriebssystem (NBS, engl.: network operating system (NOS)) hat die Aufgabe, die den Netzwerkbenutzern zur Verfügung gestellten Ressourcen zu verwalten. Dies ist im Wesentlichen die Verwaltung des von allen Benutzern gemeinsam genutzten Massenspeichers sowie die Steuerung der Schreib-/Lesezugriffe auf die Datenbestände.

Darüber hinaus werden Druckaufträge von Netzwerkbenutzern in Warteschlangen eingereiht und nacheinander auf dem gemeinsam genutzten Drucker ausgegeben. So kann ein Server für die Druckerverwaltung eingerichtet werden und ein weiterer Server die Onlinekommunikation mit externen Stationen verwalten.

Bei der Bezeichnung Netzwerkbetriebssystem handelt es sich um eine Sammlung von Systemprogrammen, die zur Steuerung eines Netzwerkes erforderlich sind.

Das Netzwerkbetriebssystem wird auf den sogenannten Server geladen und erlaubt es den Benutzern an den angeschlossenen Arbeitsstationen bzw. Clients, Nachrichten und Daten auszutauschen, sowie Dateien und Peripheriegeräte gemeinsam zu nutzen.

Im Allgemeinen bieten Netzwerkbetriebssysteme Sicherheitsvorrichtungen an, die unter anderem dafür sorgen, dass bestimmte Dateien und Zugriffsrechte gewahrt bleiben und nur Zugriffsberechtigte auch Zugriff auf sensible Datenbestände erhalten. Diese Zugriffsrechte werden in der Regel über das Benutzerprofil geregelt.

5.1.4. Standardsoftware für Netzwerke

Grundsätzlich kann in PC-Netzwerken die gleiche Standardsoftware wie auf Einzelplatzrechnern eingesetzt werden. Hierbei ist zwischen „nicht netzwerkfähiger” und „netzwerkfähiger” Software zu unterscheiden.

Kennzeichnend für netzwerkfähige Software ist, dass man gleichzeitig von verschiedenen Workstations aus mit den gleichen Programmen und Daten arbeiten kann. Die gleichzeitige Benutzung einer Datei durch mehrere Benutzer ist insbesondere im Datenbankbereich sinnvoll. Eventuelle Zugriffskollisionen werden auf Datensatzebene verhindert (Record-Locking: Der benutze Datensatz wird gesperrt).

Unter nicht netzwerkfähiger Software versteht man Produkte, die nicht für Mehrbenutzerbetrieb lizensiert sind. Hierbei ist es unerheblich, ob eventuell der mehrfache Zugriff auf die Software über das Netzwerk technisch möglich ist, da ausschließlich die Netzwerk-Lizenz aus rechtlicher Sicht die Netzwerkfähigkeit definiert.

Die Benutzung von Software-Einzelplatzversionen im Netzwerk durch einen Benutzer ist unkritisch, da hier das Netzwerk ausschließlich als Speichermedium für diese Software benutzt wird.

5.1.5. Benutzung des Netzwerkes

Das Netzwerk kann wie ein einzelner PC benutzt werden. Voraussetzung ist allerdings das Anmelden im Netzwerk. Wenn Sie sich beim Netzwerk angemeldet haben, können Sie die Ihnen zur Verfügung gestellte Software starten, Verzeichnisse anlegen und wechseln, Dateien kopieren und löschen und vieles mehr.

5.1.6. Rollen

Da in einem Netzwerk viele Benutzer gleichzeitig tätig sein können, muss die Benutzung organisiert und die Betreuung der Anwender und des Netzwerkes gewährleistet werden. Hierzu wurden in der IT-Richtlinie bestimmte Rollen eingeführt:

- *IT-Infrastrukturanbieter (IT-IA)*
  Der Infrastrukturanbieter plant, realisiert und betreibt die übergreifenden Teile der IT-Infrastruktur. Diese Rolle wird im Land Berlin durch das ITDZ wahrgenommen.

- *IT-Infrastrukturbetreuer (IT-IB)*
  Die IT-Infrastrukturbetreuung ist eine behördliche Serviceeinheit (IT-Stelle). Sie plant, realisiert und betreibt die behördenbezogenen Teile der IT-Infrastruktur (z. B. lokale Netze, Server und Endgeräte).

- *IT-Verfahrensbetreuer (IT-VB)*
  Die IT-Verfahrensbetreuung umfasst die zentrale administrative und organisatorisch-technische Betreuung des Betriebes aus fachlicher Sicht.

- *IT-Koordinatoren (IT-K)*
  Der IT-Koordinator nimmt die nicht zentral durchgeführten Aufgaben im Zusammenhang mit dem Betrieb der Fachsoftware in einer Dienststelle war und übernimmt die fachlichen Betreuungsaufgaben für seinen Bereich.

- *IT-Anwender (IT-A)*
  Der IT-Anwender ist einer bestimmten Dienststelle zugeordnet. Er hat in der Fachsoftware bearbeitende Rechte.

5.2. Netzwerktypen

Im Zusammenhang mit Netzwerken werden oft folgende Begriffe erwähnt:

- LAN (Local Area Network)
- WLAN (Wireless Local Area Network)
- VLAN (Virtual Local Area Network)
- MAN (Metropolitan Area Network)

- WAN (Wide Area Network)
- GAN (Global Area Network)

Wie die Abkürzungen schon zeigen, unterscheiden sich diese verschiedenen Netzwerktypen vor allen Dingen in der örtlichen Ausdehnung der Netze.

5.2.1. LAN (Local Area Network)

Lokale Netze sind als feste Installation dort zu finden, wo mehrere Rechner über kleine Entfernungen an einem bestimmten Ort dauerhaft vernetzt werden sollen. Für einzelne Veranstaltungen wie technikorientierte Kongresse oder LAN-Partys werden sie auch temporär aufgebaut.

Ein LAN kann man am besten dadurch beschreiben, dass seine Ausdehnung an der Grundstücksgrenze endet.

Diese Begrenzung ohne Kontakt nach außen ermöglicht eine weitgehende Freiheit bei der technischen Ausgestaltung des LAN.

Ein Lokales Netz kann mittels verschiedener Technologien aufgebaut werden. Ethernet ist heute der am weitesten verbreitete Standard. Mittlerweile erfolgt die Übertragung meist über Twisted-Pair-Kabel (CAT5 oder höher) und weitaus seltener über Glasfaserkabel. Aktuelles Ethernet deckt Datenübertragungsraten von 10 bis 1000 Mbit/s ab (entspricht maximal 125 MByte/s Datendurchsatz).

5.2.2. WLAN (Wireless Local Area Network)

Drahtlose lokale Netze nennt man Wireless LAN (WLAN). Sie werden meist über einen Standard aus der Gruppe IEEE[4] 802.11 realisiert, die zum kabelgebundenen Ethernet weitgehend kompatibel sind.

Da Funknetze nicht an Gebäude- oder Werksgrenzen halt machen, gibt es hier eine Besonderheit, die Verschlüsselungstechnik. Anfänglich wurde mit den mittlerweile als unsicher eingestuften Standards nach WEP (WEP-64 oder WEP-128) gearbeitet, die daher nicht mehr angewendet werden sollten.

Der neuere WPA-Standard gilt zurzeit noch als sicher, wenngleich man auch hier von poor-man's-security spricht, denn WLAN-Accesspoints und -Router werden unter enormem Kostendruck vermarktet.

5.2.3. VLAN (Virtual LAN)

Ein lokales Netz kann jedoch auch in mehrere LANs oder Virtual LANs unterteilt werden, um die Netzkommunikation eines einzelnen physikalischen lokalen Netzes physisch oder logisch auf zwei oder mehr VLANs aufzuteilen.

[4] nstitute of **E**lectrical and **E**lectronics **E**ngineers, ein weltweiter Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informatik mit Sitz in New York City

Zur Verbindung mehrerer getrennter LANs oder VLANs wird üblicherweise ein Router oder ein Switch mit entsprechender Funktionalität benutzt.

5.2.4. MAN (Metropolitan Area Network)

Ein Metropolitan Area Network (MAN) ist ein breitbandiges, in Glasfasertechnologie realisiertes Telekommunikationsnetz, das überwiegend in ringförmiger Struktur aufgebaut ist und die wichtigsten Bürozentren einer Großstadt miteinander verbindet. Ein MAN kann eine Ausdehnung bis zu 100 km haben.

MANs werden oft von international tätigen Telekommunikationsfirmen aufgebaut, die dann auf diese Weise verkabelte Metropolen wiederum in einem Wide Area Network (WAN) national oder sogar international in einem Global Area Network (GAN) vernetzen.

Die Berliner Verwaltung nutzt ein eigenes MAN, durch das alle Senats- und Bezriksverwaltungen, sowie nachgeordnete Behörden mit einander verbunden sind. Der Betreiber dieses MAN ist das IT-Dienstleistungszentrum Berlin (ITDZ).

5.2.5. WAN (Wide Area Network)

Ein Weitverkehrsnetz (engl. wide area network, daher auch im Deutschen oft abgekürzt WAN), auch Weitbereichsnetz, ist ein Rechnernetz, das sich im Gegensatz zu einem LAN oder MAN über einen sehr großen geografischen Bereich erstreckt.

Die Anzahl der angeschlossenen Rechner ist auf keine bestimmte Anzahl begrenzt. WANs erstrecken sich über Länder oder sogar Kontinente. WANs werden benutzt, um verschiedene LANs aber auch einzelne Rechner miteinander zu vernetzen.

Einige WANs gehören bestimmten Organisationen und werden ausschließlich von diesen genutzt. Andere WANs werden durch Internetdienstanbieter errichtet oder erweitert, um einen Zugang zum Internet anbieten zu können.

5.2.6. GAN (Global Area Network)

Unter einem Global Area Network (GAN) versteht man ein Netz das über unbegrenzte geographische Entfernungen mehrere Wide Area Networks verbinden kann. Dies kann zum Beispiel die Vernetzung weltweiter Standorte einer internationalen Firma sein. Oft wird bei einem GAN Satelliten- oder Glasfaserübertragung eingesetzt.

Der Begriff GAN wird im Vergleich zu Local Area Network (LAN) und Wide Area Network (WAN) eher selten verwendet. GAN ist nicht die direkte Bezeichnung für das Internet, da es theoretisch mehrere GANs abgeschottet und unabhängig geben kann. Das Internet ist jedoch eine globale Vernetzung ohne (maßgebliche) Unterteilungen.

So ist das Internet ein GAN aber nicht jedes GAN wird Internet genannt.

5.3. Bestandteile eines Netzwerkes

5.3.1. File-Server = Datenserver

Der File-Server ist der zentrale Rechner in einem PC-Netzwerk. Auf der Festplatte des File-Servers sind zum einen das Netzwerk-Betriebssystem und zum anderen die im Netzwerk betriebenen Softwareprodukte installiert. Dort werden auch die gemeinsam genutzten Daten abgelegt.

Der File-Server hat außerdem die Aufgabe, die benötigten Dateien an die einzelnen Arbeitsstationen zu verteilen und dabei den Netzwerkbetrieb zu überwachen. Ebenso werden Druckaufträge sowie Zugriffsrechte auf einzelne Dateien vom File-Server verwaltet.

Aufgrund der umfangreichen Aufgaben kommt als File-Server nur ein sehr leistungsfähiger Rechner in Frage, der über eine große Festplattenkapazität verfügen muss.

In größeren PC-Netzwerken ist darüber hinaus auch der Einsatz mehrerer File-Server denkbar und sinnvoll. Außerdem kommen auch Mail-Server (Nachrichten-Server), Print-Server (Druck-Server) etc. zum Einsatz, wenn dies erforderlich ist.

5.3.2. Workstation

Workstations sind alle Rechner im Netzwerk, die sich der Plattenkapazität des File-Servers bedienen. Als Workstation werden Personal-Computer bezeichnet, die nicht unbedingt eine eigene Festplatte haben müssen, da die Datenhaltung zentral auf dem File-Server stattfindet.

Eine Sonderform von Workstation ist die „diskless” oder „medialess”-Workstation, was bedeutet, dass weder ein Diskettenlaufwerk noch eine Festplatte vorhanden ist. Die Workstation bekommt in diesem Fall ihr Betriebssystem direkt von der Festplatte des File-Servers.

Umgekehrt ist es aber auch möglich, eine Workstation im Einzelbetrieb zu benutzen und nur hin und wieder in das Netzwerk einzufügen. In diesem Fall ist natürlich eine Ausstattung dieser Workstation mit Diskettenlaufwerk und Festplatte sinnvoll, man hat also wieder einen PC.

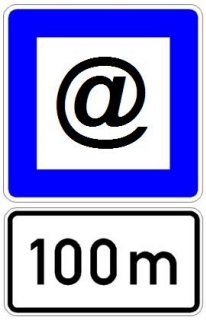
5.3.3. Netzwerkkarten

Die Leistung eines Netzwerkes hängt erheblich von den eingebauten Netzwerkkarten ab. Die Karten unterscheiden sich zum Teil recht erheblich in der Größe und auch in der Leistungsfähigkeit.

5.3.4. Netzwerk-Kabel

Die Kabel in den Netzwerken sind immer direkt von den gewählten Netzwerkkarten abhängig. Die Qualität kann von zweiadrigem Telefondraht (Twisted Pair für Ethernet) bis zu hochwertigem Spezialkabel (IBM Token Ring) reichen.

5.4. Internet



Das Internet (wörtlich etwa „Zwischennetz“ oder „Verbundnetz“, engl.: interconnected: „miteinander verbunden“ und networks: „Netzwerke“) ist ein weltw$eites Netzwerk bestehend aus vielen Rechnernetzwerken, um weltweit Daten auszutauschen. Es ermöglicht die Nutzung der Internetdienste wie Telefonie, WWW, E-Mail und Radio.

Im Prinzip kann dabei jeder Rechner weltweit mit jedem anderen Rechner verbunden werden.

Der Datenaustausch zwischen den einzelnen Internet-Rechnern erfolgt über die technisch normierten Internetprotokolle.

Umgangssprachlich wird „Internet“ häufig synonym zum World Wide Web verwendet, da dieses im Gegensatz zu anderen Diensten nur über das Internet erreichbar ist. Dies ist der meistgenutzte Internetdienst, da andere Dienste wie Telefonie, Fernsehen und Radio meist noch über andere Netzwerke genutzt werden.

Das Internet ging aus dem 1969 entstandenen Arpanet hervor, einem Projekt der Advanced Research Project Agency (ARPA) des US-Verteidigungsministeriums. Es wurde zur Vernetzung von Universitäten und Forschungseinrichtungen benutzt. Ziel des Projektes war zunächst, die knappen Rechenkapazitäten sinnvoll zu nutzen, erst in den USA später weltweit. Die anfängliche Verbreitung des Internets ist eng mit der Entwicklung des Betriebssystems Unix verbunden. Nachdem das Arpanet 1982 TCP/IP adaptierte, begann sich auch der Name Internet durchzusetzen.

Nach einer weit verbreiteten Legende bestand das ursprüngliche Ziel des Projektes vor dem Hintergrund des Kalten Krieges in der Schaffung eines verteilten Kommunikationssystems, um im Falle eines Atomkrieges eine störungsfreie Kommunikation zu ermöglichen. In Wirklichkeit wurden vorwiegend zivile Projekte gefördert, auch wenn die ersten Knoten von der Advanced Research Projects Agency (ARPA) finanziert wurden.

Die wichtigste Applikation in den Anfängen war die E-Mail. Bereits 1971 überstieg das Gesamtvolumen des elektronischen Mailverkehrs

das Datenvolumen, das über die anderen Protokolle des Arpanet2[5], das Telnet und FTP abgewickelt wurde.

Rasanten Auftrieb erhielt das Internet seit 1993 durch das World Wide Web, kurz WWW, als der erste grafikfähige Webbrowser namens Mosaic veröffentlicht und zum kostenlosen Download angeboten wurde.

Das WWW wurde 1989 im CERN (bei Genf) von Tim Berners-Lee entwickelt. Schließlich konnten auch Laien auf das Netz zugreifen, was mit der wachsenden Zahl von Nutzern zu vielen kommerziellen Angeboten im Netz führte. Der Webbrowser wird deswegen auch als die „Killerapplikation" des Internet bezeichnet. Das Internet ist ein wesentlicher Katalysator der Digitalen Revolution.

1990 beschloss die US-amerikanische National Science Foundation, das Internet für kommerzielle Zwecke zu nutzen, wodurch es über die Universitäten hinaus öffentlich zugänglich wurde.

Neue Techniken verändern das Internet und ziehen neue Benutzerkreise an: IP-Telefonie, Groupware wie Wikis, Blogs, Breitbandzugänge (zum Beispiel für Vlogs und Video-on-Demand), Peer-to-Peer-Vernetzung (vor allem für File Sharing) und Online-Spiele (z. B. Rollenspiele, Egoshooter, …).

Das rasante Wachstum des Internets sowie Unzulänglichkeiten für immer anspruchsvollere Anwendungen bringen es möglicherweise in Zukunft an seine Grenzen. Deshalb haben inzwischen Forschungsinitiativen begonnen, das Internet der Zukunft zu entwickeln.

5.5. Intranet

Ein Intranet ist ein organisations- oder unternehmensinternes, nichtöffentliches Rechnernetzwerk, das auf den gleichen Techniken (TCP/IP, HTTP) und Anwendungen wie das Internet basiert und den Mitarbeitern einer Unternehmung oder Organisation als Informations-, Kommunikations- und Anwendungsplattform zur Verfügung steht. Innerhalb eines Intranets können auch Verzeichnisdienste zur Verfügung gestellt werden.

Das Land Berlin setzt für die interne Kommunikation und den Datenaustausch ein Intranet ein.

Informationsbereitstellung

Aus den Zielen des Informationsmanagements lässt sich die Forderung ableiten, die Information, Kommunikation und Daten als wichtigen Faktor zur Erfüllung der von der Organisation angestrebten Ziele

[5] Das Arpanet *(Advanced Research Projects Agency Network)* wurde ursprünglich im Auftrag der US-Luftwaffe ab 1962 von einer kleinen Forschergruppe unter der Leitung des Massachusetts Institute of Technology und des US-Verteidigungsministeriums entwickelt. Es ist der Vorläufer des heutigen Internets.

zu betrachten. Dies führt zur Betrachtung der Informationsfunktion nicht nur als Unterstützungsfunktion für andere betriebliche Funktionen, sondern als gleichberechtigte Unternehmensfunktion. Die daraus abgeleitete Notwendigkeit, allen relevanten Usern aufbereitete Daten aus den bestehenden Quellen zu liefern, stellt eine zentrale Aufgabe des Informationsmanagements dar. Ein Intranetportal stellt dafür eine geeignete Methode dar.

Benutzerbeteiligung

Um die Beteiligung von Mitarbeitern zu erreichen, bietet die Informations- und Kommunikationstechnologie zahlreiche Möglichkeiten, die sehr genau auf die jeweiligen Benutzer- und Organisationsziele zugeschnitten eingesetzt werden können. Dazu zählen unter anderem Wikis, Blogs, Chaträume, Foren, Online-Besprechungen, Videokonferenzen und vieles mehr.

Als sehr sinnvoll erweist sich die Möglichkeit der asynchronen, standortunabhängigen Kommunikation. So werden unter anderem Fachforen zu verschiedenen Themen eröffnet, in denen sich alle berechtigten User des Intranetportals austauschen können. Zu jedem im Intranetportal veröffentlichten Beitrag können Diskussionen geführt werden. Daraus entstehen oftmals Wissensgemeinschaften, welche den Inhalt des Intranetportals diskutieren und somit neue Inhalte erarbeiten können.

Die Nutzung dieser Technologien ist in einem ständigen Wachstum begriffen; die Akzeptanz der User und deren Bereitschaft von sich aus Inhalte für das Intranetportal beizusteuern steigt stetig.

Plattformunabhängige Interaktion

Besonders in vielschichtigen Organisationen, in denen mehrere User auf verschiedenen Plattformen arbeiten, stellt ein Intranetportal ein Plattform-kompatibles Medium (gemeinsame Benutzung von Datenbasen, Vermeidung von Medienbrüchen, Verwendung elektronischer Kommunikationsmedien) oftmals über Zeitzonen hinweg (asynchrone Kommunikation) dar.

5.6. Barrierefreiheit

Barrierefreiheit bedeutet, dass Gegenstände, Medien und Einrichtungen so gestaltet werden, dass sie von jedem Menschen unabhängig von einer eventuell vorhandenen Behinderung uneingeschränkt benutzt werden können.

5.6.1. Barrierefreies Internet/Intranet

Die modernen Technologien der Informationsverarbeitung und das Webdesign bieten eine Fülle verschiedener Technologien, um Inhalte darzustellen, die in den letzten zehn Jahren zunehmend über die reine Aufbereitung von Text hinausgehen. Ressourcenbedingt

können die Hilfsmittel, die zur Darstellung notwendig sind, oft nicht adäquat nachgeführt werden, wenn es um Randgruppen geht. Solche Maßnahmen seitens der Anbieter von Webpräsenzen, aber auch der Bereitsteller von Infrastruktur und Betriebssoftware werden ausgrenzende Mechanismen genannt.

Blinde Menschen können einen gut strukturierten Text über eine Braillezeile mit entsprechender Software (Screenreader) lesen. Bilder – oder Text, der in Bildern enthalten ist – sind für Blinde unzugänglich und sollten daher mit einem alternativen Text ergänzt werden. Frames sind kein Hindernis, wenn sie die Struktur unterstützen, beispielsweise Navigation und Inhalt trennen.

Sehschwache, insbesondere ältere Menschen, benötigen Skalierbarkeit der Schrift im Browser, um die Schriftgröße an ihre Sehleistung anpassen zu können.

Personen mit einer Farbfehlsichtigkeit, z. B. einer Rot/Grün-Sehschwäche brauchen starke Kontraste und klare Schriften sowie Kontrolle über die Farbe von Schrift und Hintergrund. Blinkende oder animierte Texte stellen eine Barriere dar.

Sehbehinderte sind bei einer Navigation die aus Bildern, Java-Applets oder Flash-Objekten besteht, benachteiligt.

Personen mit Spastiken oder anderen motorischen Störungen, die keine Maus bedienen können, müssen mit der Tastatur navigieren. Sie bewegen sich meist mit der Tabulatortaste durch die Links, Formularelemente und andere aktive Objekte auf der Seite. Damit eine Webseite gut mit der Tastatur bedienbar ist, ist es wichtig, dass die Elemente in einer sinnvollen Reihenfolge angesteuert werden und dass jederzeit deutlich erkennbar ist, welches Element gerade den Fokus hat.

Gehörlose Menschen haben oft als erste Sprache Gebärdensprache gelernt. Für sie ist die Schriftsprache eine Fremdsprache und meist schwer verständlich. Auch akustische Inhalte können von gehörlosen Menschen nicht aufgenommen werden. Sie sollten deswegen durch visuell wahrnehmbare Inhalte ersetzt oder von ihnen begleitet werden. Barrierefrei sind für sie Webseiten, die in Gebärdensprache dargestellt werden.

Menschen mit kognitiven Behinderungen haben oft Probleme, lange und umständlich formulierte Texte mit schwierigen Schachtelsätzen und Fremdwörtern sowie komplexe Navigationen zu verstehen. Deswegen ist es sinnvoll, Webseiten in so genannter „leichter Sprache“ zu verfassen oder Übersetzungen in „leichter Sprache“ anzubieten.

Viele der derzeit üblichen Content-Management-Systeme (CMS) erzeugen Seiten, die für behinderte Menschen schlecht zugänglich sind. Nur sehr wenige Systeme oder Verfahren unterstützen die Autoren mit barrierefreien Eingabemöglichkeiten.

Die Nichteinhaltung technischer Standards (z.B. korrekte Codierung von Umlauten, gültiges HTML) erzeugt Webseiten, die nur von bestimmten Browsern (z. B. Internet Explorer) korrekt dargestellt werden.

Navigation mit Hilfe von aktiven Inhalten (z.B. Javascript, Flash) schließt Nutzer aus, die die dafür relevanten Plug-ins nicht installiert haben und die aus verschiedenen Gründen keine aktiven Inhalte ausführen lassen können, dürfen oder wollen.

Web 2.0 ist der Inbegriff dynamisch aufbereiteter und interaktiv zugänglicher Informationen und stellt wohl eine informationssoziologische Innovation in ähnlichem Ausmaß wie das Internet selbst dar. Die Risiken ausgrenzender Mechanismen steigen aber entsprechend der Vielfalt der Möglichkeiten. Mit der Verbreitung von Ajax besteht die Gefahr, dass die Barrierefreiheit noch schneller ins Hintertreffen gerät. Dabei ist gerade für diesen Teil der Bevölkerung der Community-Gedanke des Web 2.0 (soziale Interaktion, die über schiere Informationsvermittlung hinausgeht) besonders interessant.

5.6.2. Grundlegende Techniken für ein barrierefreies Internet

Grundvoraussetzung für barrierefreie Internetseiten ist die Einhaltung von Webstandards (gültiges HTML/XHTML). Die geforderte strikte Trennung von Inhalt (Text, Bilder usw.) und Layout erreicht man durch den korrekten Einsatz von Cascading Style Sheets[6]. Kompromisse beim Design sind nicht nötig. Einige grundlegende Möglichkeiten:

Skalierbarkeit

Feste Schriftgrößen stellen in manchen Browsern eine Barriere dar, da sie vom Nutzer nur schwer veränderbar sind. So sollte die Maßeinheit insbesondere für Schriften, aber auch für Bereiche, Abstände usw. relativ sein (Angaben in cm oder %).

Logische Struktur

Die wichtigste Regel für barrierefreie Webseiten ist, die HTML-Elemente entsprechend ihrer Bedeutung (Semantik) einzusetzen.

Nur bei aktiviertem Webseiten-Stil (im Browser über Ansicht einstellbar) führen beide Methoden zum optisch selben Ergebnis. Die erste Version ist jedoch weitaus wirtschaftlicher: Für Layoutänderungen muss bei der korrekten Version in der CSS-Datei nur eine Regel für Überschrift 1 geändert werden und sofort sind auf allen Seiten der gesamten Website sämtliche Überschriften erster Ordnung angepasst. Bei der anderen Version müssen sämtliche Überschriften auf der Webpräsenz überarbeitet werden, was äußerst zeitaufwendig ist.

[6] Cascading Style Sheets (Abk.: CSS]) ist eine deklarative Sprache für strukturierte Dokumente. Sie wird vor allem zusammen mit HTML und XML eingesetzt

An diesem Beispiel wird deutlich, dass Barrierefreiheit weniger mit „Design“ zu tun hat, sondern eher mit dem richtigen Aufbau von (X)HTML Quelltexten.

Positiver Nebeneffekt: Suchmaschinen werten semantisch richtige und valide Webseiten auf, was sich auf ein besseres Suchergebnis auswirkt.

Wird diese Methode auf alle verwendeten HTML-Elemente angewandt und die Stil-Regeln in die externe CSS-Datei ausgelagert, so ist die barrierefreie Version der herkömmlichen deutlich überlegen, da für ein Redesign der Seite nur diese CSS-Datei ausgetauscht werden muss, ohne auch nur eine einzige Änderung im (X)HTML-Dokument vornehmen zu müssen. Somit ist Barrierefreiheit auch ein Qualitätsmerkmal für Webseiten. In den folgenden Abschnitten werden weitere Möglichkeiten dargestellt.

Positionierung von Elementen

Um Elemente auf einer Seite zu platzieren, können zum einen Tabellenkonstruktionen eingesetzt werden, zum anderen lassen sich Elemente mit Cascading Style Sheets mittels genauer Koordinaten positionieren. Durch die Nutzung von Tabellen wird der Quelltext unnötig aufgebläht, da auch Bereiche definiert werden müssen, die gar nicht genutzt werden. Mit Cascading Style Sheets müssen nur Elemente definiert werden, die auch benötigt werden. Ferner sind Überlappungen von einzelnen Elementen (Vorder- und Hintergrundelemente in verschiedenen Ebenen) möglich.

Besonders vorteilhaft ist vor allem die Unabhängigkeit der angezeigten Position von der im Quelltext. So kann im HTML-Dokument der Kopfbereich des sichtbaren Inhalts erst am Ende definiert werden. Wenn dieser z. B. mit Bannern versehen wird, welche für Nutzer mit Handicap meist eher störend sind, so werden diese am Ende des Quelltextes definiert. Somit müssen Benutzer von Screenreadern nicht erst uninteressantes „lesen“, sondern können direkt den relevanten Inhalt nutzen. Sehr sinnvoll sind auch seiteninterne Sprungmarken (Anker) wie z. B. Sprung zum Inhalt (Navigation überspringen).

Sprachwechsel

Jeder Sprachwechsel sollte kenntlich gemacht werden. Ist die Webseite zum Beispiel in deutscher Sprache gehalten, können englischsprachige Wörter wie „Screenreader“ explizit ausgezeichnet werden, etwa durch ein -Tag.

Akronyme und Abkürzungen

Auch Akronyme und Abkürzungen sollten mit den eigens dafür vorgesehen HTML-Tags definiert werden. Verwendet man das ACRONYM-Tag, so buchstabiert ein Screenreader nicht die einzelnen Buchstaben, sondern spricht das Wort nach Möglichkeit als Ganzes

aus. Im Gegensatz dazu steht das ABBR-Tag (für abbrevation, zu deutsch: Abkürzung). Hier liest der Screenreader die jeweilige Abkürzung Buchstabe für Buchstabe vor.

Beispiele:

- BITV <acronym title="Barrierefreie Informationstechnik-Verordnung">BITV</acronym>
- BITV <abbr title="Barrierefreie Informationstechnik-Verordnung"> BITV</abbr>

Bilder für Layoutzwecke

Oftmals werden Bilder nur für Layoutzwecke, nicht jedoch für die Informationsvermittlung genutzt. Um die geforderten Standards einzuhalten, also um valides HTML zu erstellen, muss man Bilder mit einem alternativen Text (ALT-Attribut) versehen. Handelt es sich bei den Bildern um grafische Elemente für das Seitenlayout, wäre ein ALT-Text jedoch z. B. für Blinde störend, weshalb er leer gelassen werden sollte. Auf die Methode, zum Ausrichten von Elementen 1x1 Pixel große transparente Grafiken zu verwenden, die dann in großer Anzahl hintereinander gesetzt werden, sollte gänzlich verzichtet und stattdessen CSS zum Positionieren eingesetzt werden.

Des Weiteren werden für die Positionierung der Bilder manchmal komplizierte Tabellenkonstrukte genutzt. Mit der Positionierung von Containern (DIVs) über CSS lassen sich diese vollständig umgehen. Dient ein Bild einzig dem Layout/Design und transportiert keine relevante Information, so sollte es als Hintergrundbild im Stylesheet (background-image) definiert werden.

Interaktive Schaltflächen per CSS

Oft werden Navigationen noch mit Hilfe von JavaScript oder mittels Plug-ins (z. B.: Adobe Flash) realisiert. Dies kann den Quelltext unnötig umfangreich machen und sperrt Benutzer aus, wenn zum Beispiel:

- deren Browser kein JavaScript unterstützen (z. B.: Lynx),
- die JavaScript-Unterstützung im Browser deaktiviert ist,
- die benötigten Plug-ins nicht installiert sind oder
- der Nutzer durch eine Behinderung nicht in der Lage ist, die Navigation wahrzunehmen oder zu bedienen.

Bei den meisten Schaltflächen im Internet werden einfach nur Hintergrundfarbe oder -bild sowie Textfarbe und -dekoration ausgetauscht. Dies ist per CSS um ein Vielfaches einfacher und der Quelltext schrumpft (Bündelung von Formatangaben in Klassen). Dies verringert natürlich auch die Dokumentengröße, wodurch zugleich das Transfervolumen kleiner und die Seite schneller geladen wird. Durch eine Ausgliederung der CSS-Angaben in eine externe Datei können weitere Verbesserungen in Bezug auf Transfervolumen und Ladezeit erreicht werden, da die Formatierungen nur einmal – und nicht bei jedem neuen Aufruf – zum User übertragen werden müssen.

Fragen zur Selbstkontrolle:

25. Was ist ein Computer-Netzwerk?
26. Welche Vorteile und Gründe für den Einsatz eines Computer-Netzwerkes gibt es?
27. Welche Begriffe werden für Netzwerkgrößen und Strukturen verwendet?
28. Was ist unter dem Begriff „Internet“ zu verstehen?

6. Umgang mit Anwendungen der Informationstechnik

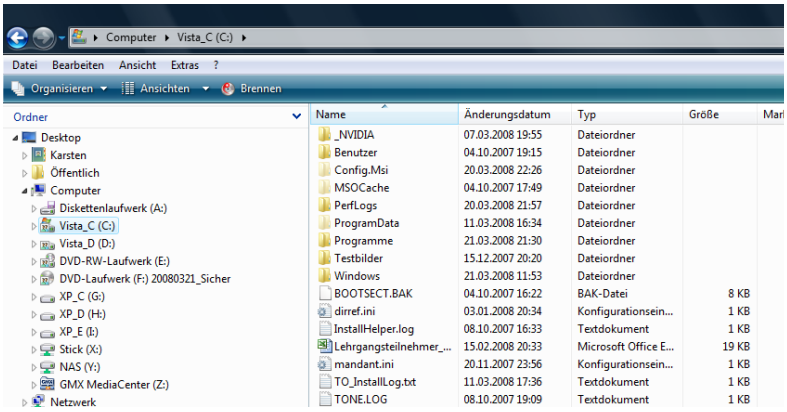
Lernziele:

Der /Die Lernende soll

- erklären können, was eine Datei ist,
- die Regeln für die Vergabe von Dateinamen wiedergeben können,
- die Begriffe „Optionsfeld“, „Dialogfeld“, „Listenkombinationsfeld“ und „Kontrollkästchen“ erläutern können,
- die Mausaktionen erläutern können.

6.1. Einführung in die Gerätebedienung

6.1.1. Windows-Explorer



Beim Windows-Explorer (auch Explorer) handelt es sich um ein Anwendungsprogramm des weit verbreiteten Computer-Betriebssystems Microsoft Windows. Oft wird er mit dem Dateimanager verwechselt, der aber nur in Windowsversionen bis Windows ME vorkommt. Der Windows-Explorer ist die Applikation, welche zu den so genannten Shellapplikationen gehört, d.h. dass der Explorer nach dem Start des eigentlichen Betriebssystems gestartet wird und die Bildschirmelemente zur Verfügung stellt. Seit Windows 95 gehören dazu die Taskleiste (mit dem Start-Knopf) sowie der eigentliche Desktop (die Oberfläche), auf welchem auch Icons liegen können, der im Prinzip aber nur einen Ordner darstellt.

Des Weiteren ist der Windows-Explorer für die Zuordnung der Dateierweiterungen zu Programmen und die Suchfunktion zuständig. Daneben verwaltet er die Laufwerke (zum Beispiel auch den Autostart).

Das eigentliche Dateimanager-Fenster ist eine spezielle Ansicht innerhalb des Windows-Explorers und keine eigene Applikation.

6.1.2. Dateipfad

In einem hierarchisch organisierten Dateisystem ist der Pfad die Abfolge der Ordner die durchlaufen werden muss, um von einer bestimmten Stelle im Dateisystem aus zu einer bestimmten Datei zu kommen.

Beispiel: /home/mustermann/briefe/liebesbriefe/

oder

c:\Dokumente und Einstellungen\Mustermann\ Eigene Dateien\liebesbriefe\.

Pfadangaben können absolut sein (wie oben genannte Beispiele), das heißt sie orientieren sich an der Wurzel des Dateisystems oder relativ, das heißt sie gehen von einer bestimmten Position in der Baumstruktur des Dateisystems zu einer anderen,

Beispiel: ../geschaeftsbriefe/,

lies: *gehe eins hoch und dann in den Ordner „geschaeftsbriefe"*.

6.1.3. Ordnerstruktur

Ordnerstruktur wird die logische Gestalt der Dateisysteme, die über Verzeichnisse verfügen, eines Rechners genannt. Üblich ist eine Baumstruktur, die bei einer Wurzel (engl. „root“) beginnt und sich dann beliebig verzweigt.

In jeder Ebene des Baumes können sowohl Dateien als auch Ordner liegen, letztere bilden die nächste Ebene des Baumes. Name und Position jeder Datei kann durch eine entsprechende Pfadangabe spezifiziert werden, die an der Wurzel beginnt und alle zu durchlaufenden Ordner auflistet.

Das Betriebssystem Microsoft Windows vergibt für jedes Dateisystem einen eigenen Laufwerksbuchstaben, so dass mehrere Bäume nebeneinander existieren.

6.1.4. Begriff “Datei”

Als Dateien werden alle geordneten Ansammlungen von maschinenlesbaren Daten bezeichnet. Man unterscheidet zwischen Datendateien und Programmdateien.

Datendateien sind Ansammlungen numerischer oder alphanumerischer Zeichen, die für die Auswertung durch ein Programm aufbewahrt werden sollen (z. B. Textzeichen eines Briefes). Programmdateien sind Ansammlungen von Befehlen in Programmiersprachen.

6.1.4.1. Dateinamen

Ein Dateiname identifiziert eine Datei auf einem Datenträger oder bei einer Datenübertragung. Meist wird eine Datei zusätzlich durch einen Verzeichnisnamen charakterisiert.

Ein Dateiname kann – abhängig vom jeweiligen Betriebssystem – aus mehreren Teilen bestehen. Die einzelnen Teile sind durch bestimmte Zeichen, die in der Regel nicht Teil des Dateinamens sein können, getrennt.

Die maximale Länge eines Dateinamens wird sowohl durch das Betriebssystem als auch durch das Dateisystem des Datenträgers begrenzt. So können etwa auf einer CD-ROM bei Verwendung des Joliet4-Dateisystems maximal 64 Zeichen genutzt werden.

Einige Betriebssysteme machen den Typ einer Datei von der Dateiendung abhängig, andere arbeiten ohne diese Konvention.

Ein Unterschied zwischen MS-Windows und Linux/Unix besteht darin, dass Windows bei Dateinamen nicht zwischen Groß- und Kleinschreibung unterscheidet, während Unix dies tut (z. B. bezeichnen dort Haustuer.txt und hausTuer.txt unterschiedliche Dateien).

Unter Windows (Windows 95, 98, ME, NT, 2000, XP, Vista) besteht ein Dateiname aus dem Namen, einem Punkt und einer Erweiterung, die den Dateityp festlegt.

Folgende Zeichen sind nicht im Dateinamen zugelassen:

< > ? " : | \ / *

Auch das Leerzeichen ist unzulässig. Anstelle von Leerzeichen wird üblicherweise der Unterstrich verwendet.

6.1.4.2. Jokerzeichen

Jokerzeichen (engl. Wildcard für die Spielkarte „Joker“) ist ein Fachausdruck aus dem Computerbereich und bezeichnet einen Platzhalter für andere Zeichen.

Viele Kommandozeileninterpreter und andere Programme erlauben den Einsatz solcher Platzhalter, um beispielsweise Gruppen von Dateien oder Dateien deren Namen man nicht genau kennt, anzusprechen. Auch Suchfunktionen in Texteditoren kennen derartige Platzhalter.

Vielfach verwendete Platzhalter sind:

- das Fragezeichen (?) für genau ein beliebiges Zeichen,
- das Sternchen (*) für eine beliebige Zeichenfolge,
- das Prozentzeichen (%) für beliebig viele (auch null) Zeichen,

- das Nummernzeichen (#) für einen numerischen Wert.

Eine Suche nach „?aus“ findet alle Zeichenketten, die auf „aus“ enden und davor einen beliebigen Buchstaben haben; Beispiele wären „haus“, „Haus“, „Maus“ und „raus“.

Die Suche nach „*aus“ liefert dagegen auch etwa „heraus“.

6.1.5. Dialogfeld

Als Dialogfenster, Dialogfeld, Dialogbox oder einfach Dialog bezeichnet man spezielle Fenster in grafischen oder zeichenorientierten Benutzerschnittstellen.

6.1.6. Klicken

Im Wesentlichen unterscheidet man drei verschiedene Mausaktionen:

- Der **Klick** bezeichnet das Drücken und sofortige Loslassen der Maustaste ohne zwischenzeitlich die Maus zu bewegen.

- Ein **Doppelklick** ist das zweimalige Drücken der Maustaste kurz hintereinander. Die Maus bleibt dabei ruhig. Manche Programme unterstützen auch mehr als zwei direkt aufeinanderfolgende Klicks (Drei- bis Fünffachklicks). Aufgrund der schwierigen Ausführung haben sich letztere aber nicht durchgesetzt.

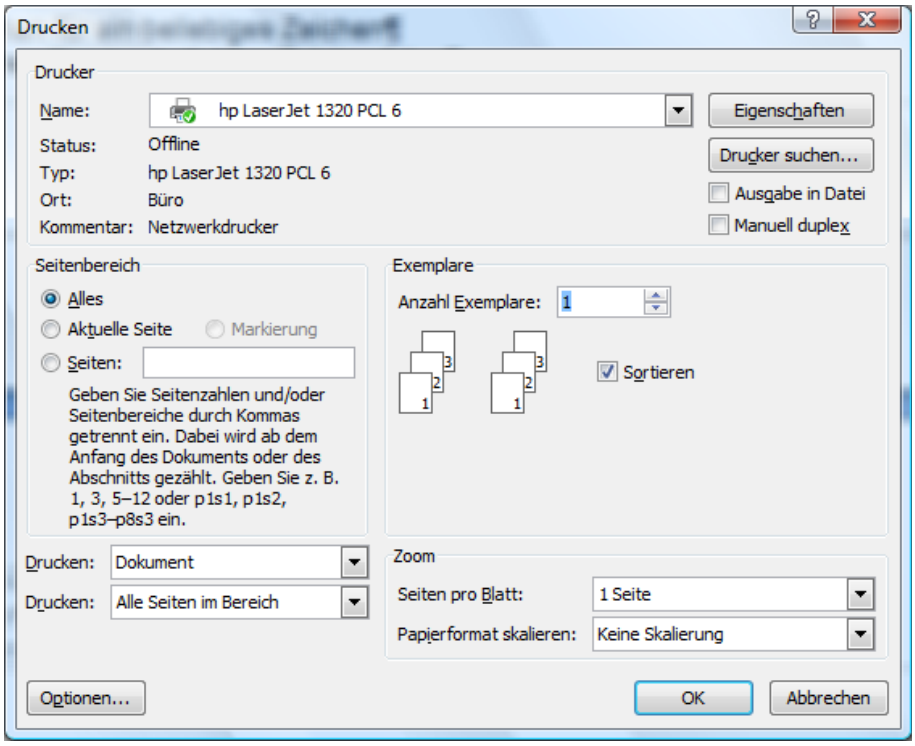
  Bei den meisten Betriebssystemen ist der Zeitabstand einstellbar, in der die zweite Tastenbetätigung erfolgen muss, um als Doppelklick akzeptiert zu werden. Manchmal ist auch ein Schwellwert einstellbar, wie weit sich die Maus zwischen den beiden Klicks bewegen darf, da sich bei hochempfindlichen Mäusen ein vollkommener Stillstand kaum noch realisieren lässt.

- **Ziehen** bedeutet, dass die Maustaste heruntergedrückt und dort gehalten wird, während die Maus bewegt wird. Erst am Ende dieses Ziehvorgangs wird die Taste losgelassen (für Aktionen wie Drag & Drop oder das Markieren von Text).

Weitere Mausaktionen sind:

- **Rechtsklick** ist der Klick der rechten Maustaste und wird synonym für Funktionen der zweiten Maustaste verwendet. Bei Linkshändern ist das der „Linksklick“ und öffnet in beiden Fällen üblicherweise ein Kontextmenü.

Dialogfeld “Drucken”



In der Regel sind Dialogfenster formularartig aufgebaut und bieten nur begrenzte Eingabemöglichkeiten. Dazu werden meist Standard-Widgets5 wie Textfelder, Kontrollkästchen (Checkboxes) und Optionsfelder (Radiobutton) verwendet.

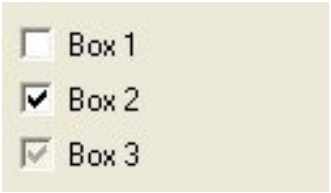
Am rechten unteren Rand enthalten Sie Schaltflächen wie „OK“ oder „Abbrechen“, mit denen der Benutzer seine Eingaben bestätigen oder verwerfen und das Dialogfenster schließen kann.

Einfache Dialogfenster, sogenannte Message Boxes, enthalten lediglich einen Frage- oder Hinweistext und eine oder mehrere Schaltflächen, etwa „Ja“ und „Nein“ zum Beantworten einer Frage.

6.1.6.1. Kontrollkästchen

Checkbox (engl. für Auswahlkasten, Kontrollkästchen) ist ein Standardelement einer graphischen Software-Benutzungsoberfläche (GUI). Eine Checkbox hat in den meisten Fällen zwei, seltener drei Zustände:

- Zustand 1: Nicht markiert (falsch)
- Zustand 2: Markiert (wahr)
- Zustand 3: Nicht aktiviert



Mit einer Checkbox werden häufig Ja/Nein-Fragen (Optionen) beantwortet und es ist üblich, die Auswahlbedingung nicht als Frage zu formulieren; also nicht:

- „Akzeptieren Sie die AGB?“ sondern „Ich akzeptiere die AGB.“

Mit jedem Mausklick auf die Checkbox kann ihr Zustand zwischen markiert (Zustand 2) und nicht markiert (Zustand 1) hin und her gewechselt werden. In seltenen Fällen kann sie auch deaktiviert werden (Zustand 3).

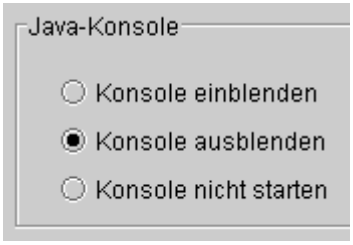
Der dritte Zustand wird nur in Sonderfällen erreicht, z. B. wenn eine Auswahl an einer anderen Stelle die Darstellung beeinflusst und folgendermaßen dargestellt:

Checkbox nicht anwählbar/editierbar und je nach Vorauswahl markiert oder nicht markiert (z. B. Feld hellgrau hinterlegt, die Vorauswahl bleibt sichtbar) und die Box reagiert nicht auf den Mausklick.

Checkbox nicht aktiviert (die Checkbox verschwindet oder das Feld wird z. B. dunkelgrau hinterlegt, so dass die Vorauswahl nicht erkennbar ist) und die Box reagiert nicht auf den Mausklick.

6.1.6.2. Optionsfeld

Ein Optionsfeld (auch Radiobutton, selten auch Mehrfachoptionsfeld oder Optionsschaltfläche genannt) ist ein Standardelement einer graphischen Benutzeroberfläche (GUI). Er kann zwei Zustände annehmen: markiert und nicht markiert.

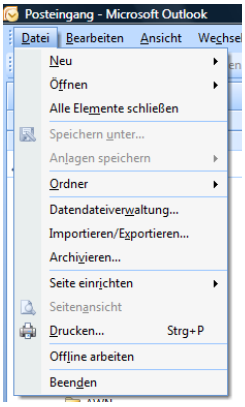


Im Gegensatz zur Checkbox kann von mehreren Radiobuttons einer Gruppe immer nur einer markiert werden. Auf diese Weise kann eine Auswahl aus mehreren Optionen getroffen werden.

Der Name Radiobutton leitet sich vom Verhalten ähnlich den Stationstasten zur Senderwahl an älteren Radiogeräten ab. Wird eine Taste gedrückt, so springt die andere wieder heraus.

6.1.6.3. Listenkombinationsfeld

Ein Listenkombinationsfeld (auch Drop-down-Liste) ist ein Element einer grafischen Benutzeroberfläche, welches durch eine Benutzeraktion (z. B. Mausklick auf eine zugehörige Schaltfläche) ein „nach unten heraus fallendes“ Listenfeld sichtbar macht. Der Ausdruck ist vom englischen Begriff „drop-down list“ abgeleitet, wobei „to drop down“ im Deutschen mit herunter-, hinunter- bzw. hinabfallen übersetzt wird.



Fragen zur Selbstkontrolle:

29. Was ist eine Datei?
30. Welche Regeln für die Vergabe von Dateinamen unter dem Betriebssystem MS-DOS kennen Sie?
31. Was sind Jokerzeichen?
32. Erklären Sie, was der Unterschied zwischen einer Optionsschaltfläche und einem Kontrollkästchen ist.
33. Was versteht man unter einem Listenkombinationsfeld?
34. Was ist ein Dialogfeld?

7. Organisatorische und rechtliche Regelungen

Lernziele:

Der /Die Lernende soll

- den Geltungsbereich des Tarifvertrags Infotechnik wiedergeben,
- was unter Mitbestimmung- und Mitwirkungsrechten des Personalrates zu verstehen ist,
- die Pflichten der Arbeitgeber zur ergonomischen Arbeitsplatzausstattung nennen können,
- die gesundheitlichen Probleme, die bei einer dauerhaften Tätigkeit am Computer auftreten können, aufzählen können,
- die Aspekte nennen können, die bei einer ergonomischen Betrachtung eines IT-Arbeitsplatzes zu beachten sind.

7.1. Tarifvertrag Infotechnik

Erster Tarifvertrag zur Änderung des Tarifvertrages vom 23. März 1989 über die Arbeitsbedingungen von Arbeitnehmern auf Arbeitsplätzen der Informationstechnik (in der Fassung des 2. Änderungstarifvertrages vom 18. Oktober 1996).

Der Wortlaut des gesamten Tarifvertrages kann nachgelesen werden:

http://www.berlin.de/hpr/rechtsgrundlagen/infotechnik.html#2

7.1.1. Geltungsbereich[7]

§ 1 TV-Infotechnik

Dieser Tarifvertrag gilt für alle Arbeitnehmer der Mitglieder des VAdöD[8] Berlin und der AV Berlin[9] auf die der BAT, der BAT-O, der BMT-G, der BMT-G-O oder ein Tarifvertrag wesentlich gleichen Inhalts angewendet wird und die auf Arbeitsplätzen mit Geräten der Informationstechnik eingesetzt sind oder werden (Bedienungskräfte).

7.1.2. Begriffsbestimmungen

Nach § 2 des TV-Infotechnik sind Geräte der Informationstechnik Bildschirmgeräte aller Art und Datenverarbeitungsanlagen, die auf elektronischem Weg Zeichen

[7] Anmerkung: zum Redaktionsschluss lag noch keine Neufassung des Tarifvertrages Infotechnik vor, in dem die aktuellen Anpassungen aus den letzten Tarifverhandlungen (2010) eingearbeitet wurden.

[8] Verband von Arbeitgebern des öffentlichen Dienstes in Berlin

[9] Arbeitsrechtlichen Vereinigung öffentlicher Verwaltungen, Betriebe und gemeinwirtschaftlichen Unternehmungen in Berlin

- aufnehmen,
- speichern und/oder
- verarbeiten und/oder
- wiedergeben und/oder
- weitergeben können.

Als Bildschirmgerät wird jedes Gerät definiert, welches zur veränderlichen Anzeige von Zeichen oder graphischen Bildern genutzt wird. Hierunter fallen auch Textverarbeitungssysteme, Mikrofilmlesegeräte und vergleichbare Geräte. Überwachungsgeräte sind davon ausgenommen.

Weiterhin unterscheidet der Tarifvertrag drei verschiedene Arten von Arbeitsplätzen mit Geräten der Informationstechnik.

7.1.2.1. Bildschirmarbeitsplätze

§ 2, Abs. 4 TV-Informationstechnik

Bildschirmarbeitsplätze sind Arbeitsplätze, bei denen die Arbeitsvorgänge, die mit und an Bildschirmgeräten zu erledigen sind, bestimmend für die gesamte Tätigkeit der Arbeitnehmer sind. Dies ist der Fall, wenn die Arbeitnehmer mit durchschnittlich mindestens der Hälfte ihrer Wochenarbeitszeit an diesen Geräten eingesetzt werden. Bildschirmarbeiten sind alle Tätigkeiten, die fast dauernden Blickkontakt zum Bildschirm oder laufenden Blickwechsel zwischen Bildschirm und Vorlage voraussetzen.

Ein beispielhafter Arbeitsplatz hierfür ist der in den Kanzleien (Schreibkräfte).

7.1.2.2. Arbeitsplätze mit Bildschirmunterstützung

§ 2, Abs. 5 TV-Informationstechnik

Arbeitsplätze mit Bildschirmunterstützung sind alle Arbeitsplätze, bei denen mit Bildschirmgeräten gearbeitet wird, aber die Arbeitsvorgänge mit und an Bildschirmgeräten nicht bestimmend für die gesamte Tätigkeit der Arbeitnehmer sind. Hierfür ist die Bürgerberatungsstelle ein beispielhafter Arbeitsplatz.

7.1.2.3. Mischarbeitsplätze

§ 2, Abs. 6 TV-Informationstechnik

Mischarbeitsplätze sind Arbeitsplätze, an denen sowohl Arbeitsvorgänge mit und an Bildschirmgeräten als auch andere Arbeitsvorgänge zu erledigen sind. Wenn ein Arbeitnehmer an einem Bildschirmarbeitsplatz tätig ist, soll ihm nach 50-minütiger Tätigkeit eine Arbeitsunterbrechung von 10 Minuten gewährt werden.

Diese Arbeitsunterbrechung ist jedoch keine Pause, sie darf nicht an den Anfang oder das Ende der Arbeitszeit oder der Pausen gelegt und auch nicht zusammengezogen werden.

Sie ist zur Erfüllung und Erledigung anderer Aufgaben gedacht, wie z. B. dem Post holen oder für Sortierarbeiten.

Für Arbeitnehmer auf Arbeitsplätzen mit Bildschirmunterstützung gilt diese Regelung entsprechend, sofern die Tätigkeit am Bildschirm über eine fortlaufende Zeit von wenigstens zwei Stunden auszuüben ist.

7.1.3. Zusammenarbeit mit dem Personalrat

Durch § 3 TV-Infotechnik wird dem Personalrat ein Informationsrecht bezüglich der Auswahl der Arbeitsbereiche in denen IT-Technik eingesetzt werden soll, über die dafür vorgesehenen Geräte und den Einsatz sowie bei wesentlichen Änderungen der eingesetzten Verfahren und der Gestaltung der Arbeitsplätze zugebilligt.

Dieses Informationsrecht ist jedoch nur ein sehr geringes und schwaches Recht. Auch der Zusatz, dass die Unterrichtung möglichst frühzeitig erfolgen soll, damit der Personalrat an der Planung teilnehmen kann, wertet dieses Recht nicht auf. Daher greift hier nun eine andere Rechtsverordnung, das Personalvertretungsgesetz (PersVG).

Nach dem PersVG, und fast nur darauf beruft sich der Personalrat, hat er ein Mitbestimmungs- und Mitwirkungsrecht.

7.1.3.1. Mitbestimmungsrecht

Dieses Recht bezieht sich auf die Gestaltung der Arbeitsplätze, die Einführung und Anwendung technischer Einrichtungen zur Überwachung der Leistung und das Verhalten der Dienstkräfte. *§ 85 Abs. 1 Nr. 12 und 13 PersVG*

Nach Absatz 2 hat der Personalrat die Möglichkeit jeweils bei der Einführung, Anwendung, wesentlichen Änderung oder wesentlichen Erweiterung bei *§ 85 Abs. 2 PersVG*

- automatisierter Verarbeitung personenbezogener Daten der Dienstkräfte
- neuer Arbeitsmethoden im Rahmen der IuK - Technik und
- betrieblichen Informations- und Kommunikationsnetzen

mitzubestimmen.

Die Wahrnehmung des Mitbestimmungsrechtes durch den Personalrat bei der Gestaltung der Arbeitsplätze spiegelt sich z. B. durch die gemeinsame Abnahme neu eingerichteter Arbeitsplätze durch den Personalrat und den zuständigen Koordinator wieder.

7.1.3.2. Mitwirkungsrecht

Hiernach hat der Personalrat das Recht bei der Einführung grundlegend neuer Arbeitsmethoden und bei grundlegenden Änderungen von Arbeitsverfahren und Arbeitsabläufen mitzuwirken. Das Informationsrecht (§ 3 TV-Infotechnik) und das Mitwirkungsrecht (§ 90 PersVG) sind sehr schwache Rechte, da beide keine Maßnahme des Arbeitgebers verhindern können. *§ 90 PersVG*

Eine fehlende Mitwirkung oder Information des Personalrates kann kein Verfahren stoppen. Beides kann nachgeholt werden und selbst wenn dies nicht geschieht, hat es keine weitreichenden Folgen.

Anders ist dies beim Mitbestimmungsrecht (§ 85 PersVG), hier bedeutet eine fehlende Mitbestimmung (Zustimmung) des Personalrates, dass ein Verfahren nicht begonnen oder ein schon laufendes Verfahren wieder eingestellt werden muss.

Der Personalrat hat nach § 11 Abs. 3 TV-Infotechnik darüber zu wachen, dass den nachfolgend genannten Zielen durch den Arbeitgeber Rechnung getragen wird.

Das Arbeitsvermögen der an Bildschirmarbeitsplätzen eingesetzten Mitarbeiter soll gefördert und ihre Gesundheit geschützt werden. Zur Erreichung dieser Ziele sollen die Handlungs- und Entscheidungsspielräume der Mitarbeiter erweitert werden.

- Der Anteil an schematischen Arbeitsabläufen soll verringert werden.
- Die Kenntnisse und Fähigkeiten der Mitarbeiter sollen erweitert und vertieft werden.
- Die Zusammenarbeit soll verbessert werden.
- Die Möglichkeit zu sozialen Kontakten ist zu erhalten.
- Die Bedienung der Geräte ist zu erleichtern und die Belastungen für die Mitarbeiter sind möglichst gering zu halten.

7.1.3.3. Zuständigkeit des Hauptpersonalrates

Sollte ein Verfahren für mehrere Bezirke eingeführt werden oder ist dies geplant, so ist hier nicht mehr der örtliche Personalrat zuständig sondern der Hauptpersonalrat (§ 59 PersVG).

Diese Zuständigkeit ist gegeben, wenn ein Verfahren für mindestens 8 Bezirke geplant ist oder eingesetzt wird.

Den Hauptpersonalrat hat dann der Pilotbezirk (Erstanwender) zu beteiligen und zu unterrichten.

7.1.4. Ausstattung der Arbeitsplätze

Die Arbeitsplätze sind nach den Sicherheitsregeln für Büroarbeitsplätze und für Bildschirmarbeitsplätze so einzurichten, dass dem Arbeitnehmer möglichst geringe psychische und physische Belastungen entstehen.

Bei der Einrichtung der Arbeitsplätze ist weiterhin das Arbeitsschutzgesetz zu beachten und die neusten gesicherten arbeitswissenschaftlichen Erkenntnisse sind zu nutzen und anzuwenden.

Außerdem ist die Richtlinie des Rates der Europäischen Gemeinschaft (EG-Richtlinie) zu beachten. Nach der EG-Richtlinie ist eine

Arbeitsplatzanalyse durchzuführen. Hierbei festgestellte Gefahren für den Arbeitnehmer sind zu beseitigen. Weiterhin sind im Anhang der EG-Richtlinie Mindestvorschriften für

- die Geräte,
- die Umgebung und
- die Mensch-Maschine-Schnittstelle

festgelegt, die der Arbeitgeber zu beachten hat und die er erfüllen muss.

Die EG-Richtlinie gilt für Geräte und Arbeitsplätze die neu beschafft und eingerichtet werden. Bereits bestehende Arbeitsplätze waren bis spätestens Ende 1996 so auszustatten, dass sie der Richtlinie genügen.

7.1.5. Schutzbestimmungen

7.1.5.1. § 5 Abs. 1 TV-Infotechnik

Ein Arbeitnehmer, der das 55. Lebensjahr vollendet hat und auf dessen Arbeitsplatz erstmals ein PC aufgestellt werden soll, muss zu dieser Maßnahme seine Zustimmung geben.

Eine Verweigerung der Zustimmung zur Aufstellung des PCs muss jedoch nicht unbedingt die Maßnahme verhindern. Es ist im Falle einer Ablehnung der Zustimmung zu prüfen, ob die Einführung aus ökonomischen und organisatorischen Gesichtspunkten notwendig ist. Trifft dies zu, so ist der Arbeitnehmer auf einen gleichwertigen Arbeitsplatz umzusetzen.

Ist dies nicht gegeben, kann die Einführung des PCs auf diesem Arbeitsplatz bis zum Ausscheiden des Mitarbeiters verschoben werden.

7.1.5.2. § 5 Abs. 2 TV-Infotechnik

Grundsätzlich hat die Umstellung des Arbeitsgebietes auf PCs so zu erfolgen, dass es zu keiner Abwertung der tariflichen Bewertung der Stelle kommt.

Sollte dies jedoch in Einzelfällen nicht zu verhindern sein, ist der betroffene Stelleninhaber umzuschulen. Die Umschulung erfolgt mit dem Ziel, dem Arbeitnehmer seine Einstufung/Gruppierung zu erhalten. Kann das nach der Umschulung nicht erfüllt werden, weil kein geeigneter Arbeitsplatz mit der bisherigen tariflichen Bewertung vorhanden ist oder ist keine Umschulung möglich, so greift hier der Tarifvertrag über den Rationalisierungsschutz.

Durch den Tarifvertrag wird gewährleistet, dass kein Arbeitnehmer durch die Einführung von PCs oder die Veränderung der Inhalte und Aufgaben eines Arbeitsplatzes entlassen werden darf.

7.1.5.3. § 5 Abs. 3 TV-Infotechnik

Im Absatz 3 wird eine Regelung getroffen, wie zu verfahren ist, wenn ein Arbeitnehmer nicht mehr aus gesundheitlichen Gründen auf einem Bildschirmarbeitsplatz eingesetzt werden kann.

In solch einem Fall ist der Arbeitnehmer möglichst auf einen gleichwertigen Arbeitsplatz umzusetzen. Umschulungskosten, die durch die Umsetzung anfallen, trägt der Arbeitgeber. Etwaige Umschulungsmaßnahmen haben während der Arbeitszeit stattzufinden.

Diese Regelungen gelten jedoch nur, wenn die gesundheitlichen Gründe, die gegen die Arbeit an einem Bildschirmarbeitsplatz sprechen, durch die Arbeit an einem Bildschirm hervorgerufen worden sind.

7.1.5.4. § 5 Abs. 4 TV-Infotechnik

In der Schwangerschaft dürfen Mitarbeiterinnen nicht an Bildschirmarbeitsplätzen eingesetzt werden, wenn sie ein ärztliches Zeugnis vorlegen und einen Antrag auf Befreiung von der Bildschirmarbeit bei ihrer Büroleitung stellen.

Ihnen ist dann möglichst ein gleichwertiger Arbeitsplatz für die Dauer der Schwangerschaft zur Verfügung zu stellen. Die bisherige Vergütung und etwaige in Monatsbeträgen festgelegte Zulagen werden weiterhin gezahlt, auch wenn kein tariflich gleichwertiger Arbeitsplatz zur Verfügung gestellt werden kann. Für den Bewährungsaufstieg zählen diese Zeiten voll mit. Nach Beendigung der Mutterschutzfrist oder der Elternzeit soll die Mitarbeiterin auf ihren alten Arbeitsplatz zurückkehren können.

7.1.5.5. § 6 TV-Infotechnik: ärztliche Untersuchung

Vor Aufnahme der Tätigkeit an einem Bildschirmarbeitsplatz muss eine ärztliche Untersuchung der Augen stattfinden. Die Anmeldung zu dieser Untersuchung wird von der Büroleitung durchgeführt. Diese Untersuchung ist dann alle drei Jahre zu wiederholen, bei gegebenem Anlass ist sie sofort zu wiederholen.

Die Untersuchung soll von dem personalärztlichen oder betriebsärztlichen Dienst während der Arbeitszeit durchgeführt werden. Die Kosten für diese Untersuchung trägt der Arbeitgeber. Die Kosten für eine notwendige PC-Sehhilfe trägt der Arbeitgeber, sofern keine andere Stelle zuständig ist (Krankenkasse).

7.1.5.6. § 7 TV-Infotechnik: Einarbeitung, Aus- und Fortbildung

Auch eine Einarbeitung und die Ausbildung an den Geräten hat vor dem Einsatz der Bildschirmgeräte zu erfolgen.

Die vom Einsatz der Bildschirmgeräte betroffenen Mitarbeiter sind rechtzeitig und umfassend in Theorie und Praxis über die Arbeitsmethoden und ihre Aufgaben zu unterrichten.

Die Mindestdauer der Schulungen muss 20 Doppelstunden umfassen. Der Inhalt hat sich auf

- die Einführung in die IuK-Technik,
- die Einweisung in den Datenschutz und die Datensicherung,
- fachspezifische Grundlagen der eingesetzten Anwendungsprogramme,
- die fachliche Einweisung,
- praktische Übungen und
- die Handhabung der Arbeitsmittel unter ergonomischen Gesichtspunkten

zu erstrecken.

Die Schulung hat während der Arbeitszeit zu erfolgen, die Kosten trägt der Arbeitgeber. Kann die Schulung nicht während der Arbeitszeit erfolgen, so ist die Zeit der Schulung auf die Arbeitszeit anzurechnen. An der Schulung muss nicht teilnehmen, wer gleichwertige Kenntnisse nachweisen kann.

7.1.5.7. § 9 TV-Infotechnik: Leistungs- und Verhaltenskontrolle

Technische Möglichkeiten mit denen Geräte und Programme der Informationstechnik vom Hersteller angeboten werden und die sich zur Kontrolle der Leistung oder des Verhaltens der Mitarbeiter werden nicht genutzt.

Einschränkungen:

- Personenbezogene Daten der Dienstkräfte dürfen zur Datenschutzkontrolle, zur Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden.
- Sie dürfen dann aber auch nur für diese Zwecke genutzt werden.
- Allerdings können diese Daten bei Bekanntwerden von Tatsachen, die den Verdacht einer Dienst- bzw. Arbeitspflichtverletzung rechtfertigen, genutzt werden.
- Sie werden dann zur Aufklärung des Verdachts ausgewertet.

7.1.5.8. § 10 TV-Infotechnik: Einrichtung von Mischarbeitsplätzen

Bildschirmarbeitsplätze sind grundsätzlich als Mischarbeitsplätze einzurichten. Bei bestehenden Arbeitsplätzen ist zu prüfen, ob sie zu Mischarbeitsplätzen umgerüstet werden können.

Ein Mischarbeitsplatz soll so gestaltet werden, dass verschiedenartige Tätigkeiten zu erledigen sind und Bildschirmarbeit mit anderen Arbeiten durchschnittlich zu etwa gleichen Teilen wechselt.

Dieser Grundsatz ist immer einzuhalten, sofern es arbeitsorganisatorisch möglich ist.

7.2. Weitere Rechtsvorschriften

- Personalvertretungsgesetz (PersVG) vom 26.07.1974 in der gültigen Fassung
- Sicherheitsregeln für Bildschirmarbeitsplätze im Bürobereich
- Sicherheitsregeln für Büroarbeitsplätze
- Tarifvertrag über den Rationalisierungsschutz (TV Rat Ang. und TV Rat Arb.)
- Richtlinie des Rates über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten (Richtlinie 89/391/EWG)

7.3. Arbeitsplatzgestaltung

7.3.1. Ergonomie

Ein Ziel der Ergonomie ist es, handhabbare und komfortabel zu nutzende Produkte herzustellen.

Ein anderes ist die ergonomische Arbeitsgestaltung, bei der es darauf ankommt eine effiziente und fehlerfreie Arbeitsausführung sicher zu stellen und das Personal vor gesundheitlichen Schäden auch bei langfristiger Ausübung einer Tätigkeit zu schützen. Somit besitzt die Ergonomie ebenfalls große Bedeutung im Bereich des präventiven Arbeitsschutzes und für die Arbeitssicherheit.

7.3.1.1. Gesundheitliche Beeinträchtigungen

Verschiedene gesundheitliche Probleme können bei der dauerhaften Tätigkeit am Computer auftreten. Man sollte sie kennen, um entsprechende Symptome frühzeitig zu erkennen und einordnen zu können.

Sehvermögen	Studien zufolge sind keine bleibenden Augenschäden nachweisbar. Subjektiv treten jedoch Beschwerden wie veränderte Farbwahrnehmungen, Doppelsichtigkeit, Brennen und Rötungen auf, die die Leistungsfähigkeit beeinträchtigen.
Stütz- und Bewegungsapparat	Dauerhafte monotone Beanspruchungen führen zu Beschwerden. Es können Schmerzen, Muskelverhärtungen und

	Gefühle der Lahmheit auftreten. Betroffen sind vor allem Kopf, Hals, Nacken, Schultern, Rücken sowie der Unterarm und Handwurzelbereich.
Kopfschmerzen	Sie korrelieren hoch mit Beschwerden im Nackenbereich und sind die häufigste Art der aufgeführten Beschwerden.
Hautprobleme	Selten treten Hautrötungen i. V. m. Juckreiz auf.
Stress	Es können erhöhte Reizbarkeit, Depression, langanhaltende Erschöpfungsphasen, Nervosität und Konzentrationsschwäche auftreten.
Schwangerschaftsprobleme	Es existieren Hinweise auf Probleme, die mit bisherigen Studien nicht nachgewiesen werden konnten.

7.3.1.2. Bildschirme

Der Bildschirm ist die Schnittstelle zwischen Mensch und Gerät. Während acht Stunden Bildschirmarbeit wechselt Ihr Blick bis zu 30.000 mal zwischen Vorlagen und Bildschirm.

Bei der Auswahl des Bildschirmes sollte daher besonders sorgfältig auf folgende Kriterien geachtet werden.

Bildwiederholfrequenz

Die Bildwiederholfrequenz des Monitors muss mindestens 72 Hz betragen.

Zeichengröße

Die Zeichengröße muss mindestens 4 mm Höhe und 2,5 mm Breite aufweisen. Dies wird bei einer normalen Textverarbeitung mit einer Darstellung von 25 Zeilen mit 80 Zeichen pro Zeile auf einem Anzeigefeld von 13 Zoll (=33 cm) erreicht.

TCO '03

TCO '03 zertifiziert nur Kathodenstrahl- und Flachbildschirme. Die Anforderungen enthalten die Bedingungen von TCO '99. Die ursprüngliche Anforderung, dass der Monitor ein helles Gehäuse haben sollte, da dies als augenfreundlicher gilt, wurde im Oktober 2005 aufgegeben.

Allerdings schreibt das TCO Development zur Farbe des Rahmens:

"Denken Sie daran, wie der Raum aussieht, in dem der Monitor stehen soll. Wählen Sie einen Monitor mit einer neutralen Farbe in Bezug auf die Licht- und Beleuchtungsverhältnisse in seiner Umgebung. Der Monitorrahmen sollte nicht zu dunkel oder zu hell im Vergleich zu der Wand hinter dem Monitor sein."[10]

[10] http://www.tcodevelopment.com/pls/nvp/Document.ShowClean?CID=1200&MID=946

Um eine entspannte Kopfhaltung zu ermöglichen, sollte die Blicklinie um etwa 35 ° aus der Waagerechten abgesenkt werden und einen annähernd rechten Winkel mit der Bildschirmoberfläche bilden. Dies erfordert, dass der Bildschirm in der Neigung verstellbar ist und dass der Winkel der Draufsicht verändert werden kann. Außerdem ist es wichtig, dass die Sicht von allen Seiten auf den Bildschirm eine hohe Qualität aufweist.

Reflexionen

Blendungen und Spiegelungen erschweren das Erkennen der Zeichen auf dem Bildschirm. Ihre Augen müssen sich dann unnötig anstrengen. Der Bildschirm sollte neig- und drehbar sein. Häufig kann eine kleine Bewegung hier Abhilfe schaffen.

Der ideale Standort des Monitors befindet sich im rechten Winkel zum Fenster und seitlich von Deckenleuchten/Leuchtreihen. Ist dies nicht möglich, so kann auch ein schräg zum Fenster versetzter Standort (bis ca. 45°) gewählt werden. Die Oberfläche des Monitors sollte möglichst gut entspiegelt sein.

Unschärfe und Flimmern

Achten Sie besonders auf die richtige Einstellung der Bildschirmhelligkeit und des Kontrastes. Eine zu helle Einstellung kann zum unangenehmen Flimmern oder zu einem Überstrahlen der Zeichen führen. Sie ist genauso ermüdend wie eine zu dunkle Einstellung des Bildschirms.

Strahlung

Die Strahlung an Bildschirmgeräten steht häufig im Mittelpunkt des Interesses der Öffentlichkeit. Eine Gesundheitsgefährdung durch Strahlenbelastung am Bildschirm ist nach heutigem Wissensstand und nach den bisherigen Erfahrungen bei den modernen Geräten nicht zu erwarten.

Ionisierende Strahlung

Die Bildröhre arbeitet mit Elektronen, die in einem Hochspannungsfeld beschleunigt werden und beim Auftreffen auf den Leuchtstoff (Phosphor) der Bildschirminnenwand einen Lichtpunkt erzeugen. Bei diesem Abbremsvorgang entsteht auch Röntgenstrahlung (Bremsstrahlung), deren maximale Energie durch die Röhrenspannung begrenzt wird. Es handelt sich deshalb um eine extrem ”weiche” Röntgenstrahlung, die im Glas der Bildröhre nahezu vollständig bis vollständig absorbiert wird. Sie ist außerhalb allenfalls mit hochempfindlichen Messgeräten nachweisbar.

Nichtionisierende Strahlung

Zur nichtionisierenden Strahlung zählen:

- statische Felder
- elektromagnetische Felder
- Ultraschall
- Infrarot-Strahlung
- Ultraviolett-Strahlung

Bei Versuchsreihen genommene Messwerte am Arbeitsplatz (30 cm von der Bildschirmoberfläche) im Vergleich mit den entsprechenden Grenzwerten ergaben, dass die gemessenen Werte am Arbeitsplatz

in der Regel um mindestens zwei bis drei Größenordnungen unterschritten werden. Elektrische Felder sind direkt am Gerät etwas höher.

7.3.1.3. Arbeitsmedizinische Vorsorge

Das Sehvermögen von Arbeitnehmern an Bildschirm-Arbeitsplätzen ist von einem ermächtigten Arzt überprüfen zu lassen (§ 6 TV-Infotechnik).

Die Erstuntersuchung hat vor Aufnahme der Tätigkeit zu erfolgen. Nachuntersuchungen sind in dreijährigem Abstand vorzunehmen und beziehen sich in der Regel auf eine augenärztliche Untersuchung. Die Augenärztliche Untersuchung ist ebenfalls vor Aufnahme der Tätigkeit am Bildschirm durchzuführen und umfasst mindestens die folgenden Punkte:

- Nahsichtfähigkeit
- Fernsichtfähigkeit
- Aktionsverschiebung
- räumliches Sehen
- Farbsehfähigkeit

Der Arbeitgeber hat dem Beschäftigen im Rahmen der Dienstzeit die Möglichkeit einzuräumen, diese Untersuchung durchführen zu lassen und die Kosten hierfür zu übernehmen.

7.3.1.4. Beleuchtung

Die künstliche Beleuchtung muss auch bei allen Tageslichtverhältnissen gute Sehbedingungen gewährleisten und darf nicht Anlass für Direkt- oder Reflexblendung sein. Eine direkte Blendung durch Leuchten wird durch die Verwendung von so genannten Rasterleuchten verhindert.

Die Beleuchtungsstärke sollte mindestens 500 Lux betragen. Langfeldleuchten sind parallel zur Blickrichtung anzuordnen. Sehr häufig sind Blendquellen im Gesichtsfeld (Tischleuchten, Fenster).

Blendungen durch einfallendes Sonnenlicht werden durch die Verwendung von Innen- und/oder Außenjalousien bzw. Vorhängen vermieden.

7.3.1.5. Lärm

Ein Schalldruckpegel von 40 dB(A) ist anzustreben. Er darf 55 dB(A) bei höheren geistigen Anforderungen nicht übersteigen.

Der Schalldruckpegel am Arbeitsplatz ist ein Immissionswert, der alle am Arbeitsplatz eintreffenden Geräusche enthält und unter anderem über 8 Stunden gemittelt wird.

7.3.1.6. Tastaturergonomie

Ergonomische Gesichtspunkte

Ein häufig vernachlässigter Faktor ist der der Ergonomie. Eine Tastatur kann schräg geneigt, abgestuft oder gewölbt sein. Die gewölbte Tastatur gehört zu den neueren Entwicklungen; sie passt sich am besten den Fingerbewegungen beim Tippen auf den unterschiedlichen Ebenen an.

Eine flache Neigung der Tasten ist insbesondere für Handflächen angenehm, denn man kann sie auf die Tischplatte auflegen, während die Finger ohne weiteres die Tasten erreichen. Daneben gibt es auch Tastaturen, die bereits ein weit vorstehendes Gehäuse haben, so dass die Handflächen voll auf der Tastatur aufliegen können.

Sehr wichtig sind bei jeder Tastatur der Tastendruckpunkt und die Rückmeldung, auch Echo genannt. Der Druckpunkt, der Punkt von dem an die Eingabe erfolgreich getätigt ist, sollte so gewählt sein, dass versehentliches Abrutschen bei einer Taste nicht gleich zu einer Eingabe der benachbarten Taste führt, d.h. der Druckpunkt sollte etwa in der Mitte des Tastenweges liegen. Dieser Weg, auch Tastentiefgang genannt, liegt je nach Tastatur zwischen 0,8 und 9,5 mm.

Im Zeitalter der mechanischen Rechen- oder Schreibmaschinen war das Echo sekundär; man hörte ohnehin ”was die Type geschlagen hatte”. Bei der heutigen Elektronik ist dies jedoch nicht immer der Fall. Wegen der fehlenden Geräuschkulisse bei Computertastaturen kann es häufig zu fehlenden oder Doppeleingaben kommen, weil die Taste zu kurz oder zu lang gedrückt wurde. Beim Echo unterscheidet man zwischen der akustischen und taktilen (mechanischen) Rückmeldung. Entweder erfolgt mit Drücken der Taste ein kleiner Piepton oder eine gefühlsmäßige Wahrnehmung einer mechanischen Überwindung eines Kontaktes. Taschenrechner haben fast ausschließlich das taktile Echo, während die Computertastaturen das akustische Echo bzw. beides bevorzugen. Dabei kann das akustische Echo sowohl von der Tastatur selbst, als auch vom Lautsprecher des Computers kommen. Wichtig ist, dass überhaupt eine Echoart vorhanden ist, ansonsten wird das Arbeiten erheblich erschwert.

5° Neigungswinkel

8°30“ Neigungswinkel

12° Neigungswinkel

Funktionale Gesichtspunkte

Tastaturen gibt es in vielfältigen Variationen. So sieht z. B. eine Tastatur für einen Bankkassierer völlig anders aus als die einer Bürokraft. Neben freistehenden Tastaturen gibt es auch feste, d.h. im Rechnergehäuse integrierte Tastaturen. Letztere sind hauptsächlich bei tragbaren Computern zu finden, deren Tastatur gleichzeitig als

Klappdeckel funktioniert. Weiterhin kann die Tastatur bereits den gesamten Rechner beinhalten (einschließlich der Zentraleinheit). Dazu ist z. B. der legendäre C64 von der Firma Commodore zu zählen.

Die Tastatur ist in diesen Fällen relativ hoch und nicht so benutzerfreundlich. Es gibt also für verschiedene Anwendungen spezielle Tastaturen. Wenn es möglich ist, achte man auf folgende Dinge:

- flache Tastatur (höhenverstellbar)
- Tastendruck mit Echo
- große Enter- (Return-) Taste
- Funktionsblöcke möglichst räumlich getrennt

7.3.2. Arbeitsmöbel

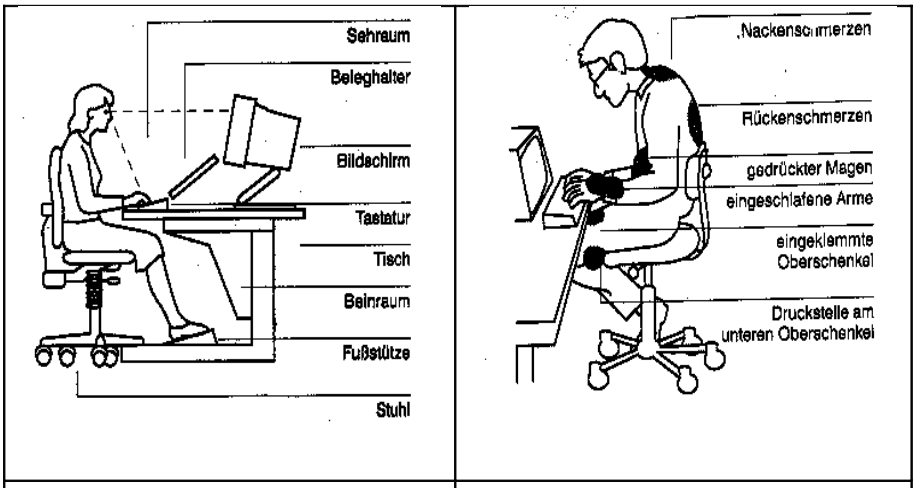
Höhenverstellbare Bürodrehstühle und Arbeitstische ermöglichen den Benutzern eine angepasste und funktionsgerechte Körperhaltung. Große durchgehende Arbeitsflächen erlauben es, Schriftstücke, Tastatur und Bildschirm den jeweiligen Anforderungen entsprechend anzuordnen.

7.3.2.1. Arbeitsstuhl

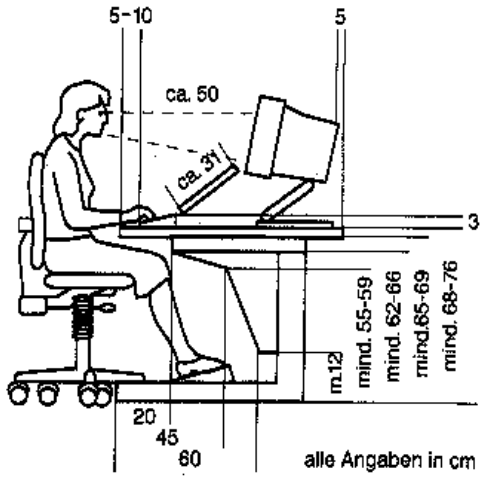
Die günstigste Sitzhaltung für die Wirbelsäule ist die aufrechte Haltung. Die Bandscheiben sind gleichmäßig belastet.

Die Sitzhöhe sollte zwischen 40 cm und 54 cm in Bezug auf den Boden einstellbar sein. Der Stuhl muss kippsicher, wegrollsicher, stolpersicher, die Sitzfläche gepolstert und der Sitz an der Vorderkante abgerundet sein. Die Anpassung der Sitztiefe durch horizontale Verstellbarkeit der Rückenlehne im Bereich zwischen 38 cm und 42 cm in Bezug auf die Sitzvorderkante sowie die Höhenverstellbarkeit der Rückenlehne (18 bis 25 cm von der Sitzfläche) müssen gegeben sein.

Richtiges Sitzen **Falsches Sitzen**



Bestandteile ergonomischer Gestaltung	Folgen physischer Beanspruchung

	durch Fehlhaltung
	

Beispiel eines ergonomisch gestalteten Bildschirmarbeitsplatzes

7.3.2.2. Arbeitstisch

Die Oberfläche des Arbeitstisches sollte einen maximalen Reflexionsgrad von 50 % aufweisen. Eine Höhenverstellbarkeit der Arbeitstische ist nicht zwingend vorgeschrieben.

Die Tischhöhe muss bei nicht höhenverstellbaren Arbeitstischen 72 cm betragen. Für höhenverstellbare Tische gelten Höhen von 68 cm bis 76 cm. (Untergrenze Schreibmaschinentisch 60 cm.)

Die Tischtiefe sollte 90 cm betragen, damit bei einem normalen Sehabstand von mindestens 50 cm kein Überstehen des Bildschirmes über die hintere Tischkante hinaus auftritt.

Die Beinraumhöhe soll mindestens 65 cm und die Beinraumbreite min. 80 cm betragen.

Am Arbeitsplatz sitzend muss der Arbeitnehmer sich mit dem Stuhl um die eigene Achse drehen können, ohne dass er an den Arbeitstisch stößt. Die Oberschenkel dürfen bei körpergerechter Anordnung nicht an die Tischplatte stoßen.

Als Ablage- und Stauraum haben sich Unterschränke auf Rollen bewährt. Die Zuleitungen zum Bildschirmgerät müssen gesichert und abgedeckt sein. Als eine hervorragende Alternative zu den höhenverstellbaren Tischen bieten sich Schwenkarme an.

Fragen zur Selbstkontrolle:

35. Für wen gilt der Tarifvertrag Infotechnik?
36. Was ist unter Mitbestimmung- und Mitwirkungsrechten des Personalrates zu verstehen?
37. Welche Pflichten muss der Arbeitgeber erfüllen?
38. Welche gesundheitlichen Probleme können bei einer dauerhaften Tätigkeit am Computer auftreten?
39. Welche Aspekte sind bei einer ergonomischen Betrachtung eines IT-Arbeitsplatzes zu beachten?

8. Datenschutz und Datensicherheit

Lernziele:

Der /Die Lernende soll

- den Sinn und Zweck des Datenschutz beschreiben können,
- das Prinzip der Datenschutz erklären können,
- die Kontrollmöglichkeiten aufzählen und erläutern können,
- Bedrohung aufzählen können, die für Daten bestehen können,
- technische und organisatorische Maßnahmen aufzählen und erklären können, die dem Schutz der Daten dienen,
- Datensicherungsmöglichkeiten aufzählen können,
- erklären können, was Viren sind,
- die bekannten Virenarten nennen und kurz beschreiben können.

8.1. Datenschutz

8.1.1. Was soll Datenschutz bewirken?

Datenschutz soll Wissen anderen gegenüber abschotten, d.h. es sollen ”Geheimnisse” bewahrt werden (z. B. Militär- oder Firmengeheimnisse). Er soll dazu beitragen, dass Barrieren und Hemmungen abgebaut werden. Das bedeutet, es soll jedem ermöglicht werden, intime Daten preiszugeben ohne dass diese dann allgemeine Verbreitung finden (z. B. Beichtgeheimnis).

Hier soll die Privatheit jedes Einzelnen sichergestellt werden. Das heißt jedem soll ermöglicht werden, einige Daten nur für sich zu behalten (z. B. Steuergeheimnis oder Bankgeheimnis). Daraus ergibt sich, dass Datenschutz ein Individualrecht ist, es gilt für natürliche Personen. Juristische Personen werden nach dem Bundesdatenschutzgesetz (BDSG) nur dann geschützt, wenn ein konkreter Personenbezug erkennbar ist.

Der Leitsatz des Datenschutzes ist:

ES GIBT KEINE FREIEN DATEN!

Alle personenbezogenen Daten, die in den Schutzbereich des Datenschutzes fallen, sind geschützt.

Denn selbst aus einer Anschrift ist es möglich, Rückschlüsse auf die Person zu ziehen.

Beispiele: a) Lieschen Morgenroth, 13437 Berlin, Oranienburger Str. 285
b) Robert Schmidt, 10701 Berlin, Bundesplatz 1
c) Rudi Pachulke, 13444 Berlin, Seidelstr. 39

- Auf den ersten Blick handelt es sich bei diesen Adressen um „normale“ Adressen. Bei näherer Betrachtung ergeben sich jedoch folgende „Besonderheiten“:

- Lieschen Morgenroth, 13437 Berlin, Oranienburger Str. 285
  Hierbei handelt es sich um die Adresse der Karl-Bonhoeffer-Nervenklinik in Berlin-Reinickendorf.

- Robert Schmidt, 10701 Berlin, Bundesplatz 1
  Dies ist tatsächlich eine ganz normale Wohnanschrift ohne Besonderheiten.

- Rudi Pachulke, 13444 Berlin, Seidelstr. 39
  Hier weiß ein Eingeweihter, dass Rudi zurzeit eine Haftstrafe in der Justizvollzugsanstalt Tegel verbüßt. Dienstwohnungen haben eine andere Anschrift.

8.1.2. Die Entwicklung des Datenschutzes

Warum ist nun aber plötzlich ein Datenschutzgesetz notwendig? Es wurden doch seit Bestehen der Verwaltung Daten von Bürgern gesammelt und verarbeitet.

Der Grund ist, dass es durch die schnelle technische Entwicklung in den Bereichen Personalcomputer, Arbeitsplatzrechner, Netzwerken, Mehrrechnersysteme, Datenfernübertragung und Datenfernverarbeitung und die daraus resultierenden Möglichkeiten und Gefahren notwendig geworden ist, die Persönlichkeitsrechte des Einzelnen unter Schutz zu stellen.

Das Persönlichkeitsrecht des Einzelnen ist dadurch gefährdet, dass durch die Technik die Möglichkeit besteht, durch verschiedene Stellen gespeicherte Daten zu kombinieren. Aus dieser Datenkombination könnte dann ein Persönlichkeitsprofil einer bestimmten Person erstellt werden.

Diese Möglichkeit gab es früher zwar auch schon, nur war die Zusammenführung aller dafür benötigten Daten wesentlich schwieriger, da alle Daten nur in Aktenform vorlagen und mühselig zusammengeschrieben werden mussten.

Deshalb wurde damals durch die Regierung auch keine Notwendigkeit für eine solche gesetzliche Regelung gesehen.

Die Notwendigkeit für eine gesetzliche Regelung des Datenschutzes wurde erst durch das Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz von 1983 erkennbar.

Dort hat das Bundesverfassungsgericht dann auch Leitsätze zur Schaffung eines Datenschutzgesetzes aufgestellt.

Leitsätze zum Urteil des Ersten Senats des Bundesverfassungsgerichts vom 15. Dezember 1983:

1. Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Artikels 2 Absatz 1 in Verbindung mit Artikel 1 Absatz 1 Grundgesetz umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.
2. Einschränkungen dieses Rechtes auf ”informationelle Selbstbestimmung” sind nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss.

Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

In diesen Leitsätzen wurde auch zum ersten mal der Begriff der ”informationellen Selbstbestimmung” erwähnt. Unter informeller Selbstbestimmung wird der Grundsatz verstanden, selbst über den Gebrauch und die Verwertung seiner persönlichen Daten zu bestimmen und informiert zu sein. Die ”informationelle Selbstbestimmung” wird aus folgenden Gründen vom Bundesverfassungsgericht8 gefordert:

> ”Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

Mit Recht auf informelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was, wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.

Um dieser Verhaltensweise des „nur nicht Auffallens“ vorzubeugen und den Einzelnen nicht zu einem, zumindest in der Öffentlichkeit ”staatstreuen Bürger” zu gestalten, wurde ein Datenschutzgesetz für notwendig erachtet und der Gesetzgeber zum Erlass eines solchen Gesetzes aufgefordert.

Das eingeforderte Gesetz, das Bundesdatenschutzgesetz (BDSG), wurde dann am 20. Dezember 1990 erlassen. Der § 1 Absatz 1 des BDSG erklärt den Zweck des Gesetzes und spiegelt die Forderung des Bundesverfassungsgerichts wieder.

”Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.”

Zur gleichen Zeit, am 17. Dezember 1990, wurde auch das Berliner Datenschutzgesetz (BlnDSG) erlassen.

Dieses, im Original ”Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung” genannte Datenschutzgesetz gilt nur für die Verwaltung und ist enger als das Bundesdatenschutzgesetz ausgelegt. Im Anhang 1 des Lehrbriefes ist der gesamte Wortlaut dieses Gesetzes abgedruckt. Die engere Auslegung ergibt sich schon aus dem Vergleich des ersten Paragraphen.

Hier heißt es im Berliner Datenschutzgesetz:

§1 Abs. 1

Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen zu regeln, um das Recht des Einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in einer anderen Rechtsvorschrift zugelassen sind (informelle Selbstbestimmung), die auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Ordnung vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

§ 1 Abs. 2

Dieses Gesetz schützt personenbezogene Daten, die von Behörden oder sonstigen öffentlichen Stellen erhoben, gespeichert, verändert, übermittelt, gesperrt, gelöscht oder sonst genutzt werden.

Zum einen wird hier festgelegt, dass das Gesetz nur für die Verwaltung gilt, und zum anderen wird auch eine mögliche Bedrohung der verfassungsmäßigen Ordnung (Gewaltenteilung) geschützt. Ein weiterer Punkt für die engere Auslegung ist der Schutz von Daten verstorbener Personen im Berliner Datenschutzgesetz.

Nach dem Bundesdatenschutzgesetz sind nur die Daten von natürlichen Personen geschützt. Mit seinem Ableben verliert man den Status einer natürlichen Person und wird zur Sache. Die Daten der dann als Sache zu betrachtenden verstorbenen Person schützt aber auch das Berliner Datenschutzgesetz.

Als Grundsatz über die Schutzwürdigkeit von Daten Verstorbener gilt, je länger eine Person tot ist, um so weniger schützenswert sind ihre Daten.

Die Anwendung der beiden Rechtsvorschriften ist in Berlin so geregelt, dass das Berliner Datenschutzgesetz für alle Landesbehörden Anwendung findet und das Bundesdatenschutzgesetz für alle Bundesbehörden in Berlin und die privaten Datenverarbeiter angewendet wird.

8.1.3. Begriffsbestimmungen

8.1.3.1. Personenbezogene Daten

§ 4 Abs. 1 Berliner Datenschutzgesetz (BlnDSG)

Personenbezogene Daten sind die Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Entsprechendes gilt für Daten über Verstorbene, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.

8.1.3.2. Datenverarbeitende Stelle

§ 4 Abs. 3 Nr. 1 Satz 1 BlnDSG

Eine datenverarbeitende Stelle ist jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt.

Merke:

Auch eine Behörde unterteilt sich in mehrere datenverarbeitende Stellen und ist somit zueinander Dritter. Sie übermittelt also Daten untereinander (z. B. im Bezirk das Wohnungsamt zum Sozialamt).

8.1.3.3. Dritte

§ 4 Abs. 3 Nr. 3 BlnDSG

Dritter ist jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen oder Stellen, die in den Fällen der Nummer 1 im Geltungsbereich des Grundgesetzes im Auftrag tätig werden.

Merke:

Jede nicht direkt beteiligte Person oder Stelle ist Dritter.

8.1.3.4. Datei

§ 4 Abs. 3 Nr. 5 BlnDSG

Eine Datei ist eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei) oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei).

8.1.3.5. Akten

Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage, Bild- oder Tonträger. *§ 4 Abs. 3 Nr. 6 BlnDSG*

Merke:

Das Datenschutzgesetz gilt für alle computergestützten Dateien und Akten.

8.1.3.6. Datenverarbeitung

Die Datenverarbeitung selbst ist das:

Erheben	das Beschaffen von Daten.
Speichern	das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger.
Verändern	das inhaltliche Umgestalten gespeicherter Daten, ungeachtet der dabei angewandten Verfahren.
Übermitteln	das Bekanntgeben gespeicherter oder durch die Datenverarbeitung gewonnener Daten an Dritte in der Weise, dass die Daten durch die speichernde Stelle weitergegeben oder zur Einsichtnahme oder zum Abruf bereitgehalten werden.
Sperren	das Verhindern weiterer Verarbeitung der gespeicherten Daten.
Löschen	das unkenntlich machen gespeicherter Daten.
Nutzen	jede sonstige Verwendung personenbezogener Daten.

8.1.4. Prinzip des Datenschutzes

Der Datenschutz baut auf die Zulässigkeit der Datenverarbeitung auf. D.h. als erstes ist zu prüfen, ob überhaupt Daten verarbeitet werden dürfen.

Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn es das Bundesdatenschutzgesetz oder eine andere Rechtsvorschrift ausdrücklich erlaubt oder der Betroffene schriftlich eingewilligt hat. *§ 6 Abs. 1 BlnDSG*

Ist dies gegeben, unterliegen auch die weiteren Punkte der Datenverarbeitung besonderen Richtlinien.
So ist das Speichern und Verändern personenbezogener Daten nur zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist. *§ 9 BlnDSG*

Auch die Übermittlung personenbezogener Daten an Behörden ist nur dann zulässig, wenn sie zur rechtmäßigen Erfüllung der in der *§ 12 Abs. 1 BlnDSG*

Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist.

§ 19 Abs. 2 BlnDSG

Die Behörde hat außerdem unverzüglich nach der ersten Speicherung dem Betroffenen:

- die Art der von ihm gespeicherten personenbezogenen Daten,
- die Aufgabe, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist,
- den betroffenen Personenkreis,
- die Stellen, an die sie personenbezogene Daten regelmäßig übermitteln und
- die Art der zu übermittelnden Daten

bekannt zu geben.

Diese Zulässigkeit wird nun durch verschiedene Punkte kontrollierbar und für den Betroffenen übersichtlicher und nachvollziehbar:

- Durch den Betroffenen, dem Rechte zur Kontrolle und Schutz gewährt werden.
- Durch Pflichten für die datenverarbeitende Stelle.
- Durch ein Gebot für die datenverarbeitende Stelle, zur Durchführung von technisch-organisatorischen Maßnahmen zur Sicherung sowie bei der Verarbeitung und dem Umgang mit bereits verarbeiteten Daten.
- Durch eine dreistufige Kontrolle der datenverarbeitenden Stelle.

8.1.5. Kontrollmöglichkeiten

8.1.5.1. Selbstkontrolle

Dem Betroffenen werden diverse Rechte gewährt, um die Verarbeitung seiner Daten zu kontrollieren und ggf. zu unterbinden.

Recht auf Auskunft und auf Einsicht (§ 16 Abs. 1 BlnDSG)

Im Einzelnen sind dies das Recht auf Auskunft und auf Einsicht (§ 16 Abs. 1 BlnDSG).

Dieses Recht gewährleistet, dass jeder Auskunft über die über ihn gespeicherten Daten verlangen kann. Das Problem ist, bei welchen Behörden man gespeichert sein könnte. Alle Behörden zu befragen, ist zu langwierig und kostspielig.

Zu diesem Zweck gibt es in jeder datenverarbeitenden Stelle ein Dateienverzeichnis, in das eingesehen werden kann und dann anhand der Information selektiert werden kann, wo man meint gespeichert zu sein.

Recht auf Benachrichtigung (§ 16 Abs. 2 BlnDSG)

Weiterhin hat der Betroffene das Recht auf Benachrichtigung (§ 16 Abs. 2 BlnDSG).

Hierbei ist festgelegt, dass der Betroffene noch vor der Speicherung seiner Daten davon unterrichtet wird. Gleiches gilt für die Übermittlung seiner Daten.

Dies geschieht meistenteils schon bei der Erhebung der Daten mittels des Satzes, ”Ihre Daten werden auf elektronischem Weg verarbeitet.” Erhebt man gegen diesen Passus keine Einwände, so gilt dies als Zustimmung.

Recht auf Berichtigung, Sperrung und Löschung von Daten (§ 17 Abs. 1 bis 3 BlnDSG)

Weitere Rechte sind das Recht auf Berichtigung, Sperrung und Löschung von Daten (§ 17 Abs. 1 bis 3 BlnDSG).

Das Recht auf Berichtigung ist dann anzuwenden, wenn personenbezogene Daten rechtmäßig, aber fehlerhaft gespeichert sind. Um obiges Beispiel weiterzuverwenden:

In diesem Fall habe ich als Betroffener das Recht, die Behörde zur Berichtigung aufzufordern, und sie muss dieser Aufforderung nachkommen.

Das Recht auf Sperrung personenbezogener Daten kommt dann zum Tragen, solange nicht genau geklärt ist, ob gespeicherte Daten falsch sind oder nicht.

Beispiel:

Die Daten des Betroffenen werden bei der Beantragung eines Wohnberechtigungsscheines gespeichert, aber das Geburtsdatum wird falsch eingegeben.

Sobald der Betroffene dies festgestellt und der Behörde mitgeteilt hat, sperrt diese die Daten zur weiteren Ver- und Bearbeitung. Die Daten bleiben so lange gesperrt, bis der Betroffenen durch Vorlage der Geburtsurkunde oder des Ausweises sein richtiges Geburtsdatum nachgewiesen hat.

Sollten allerdings Daten über eine eventuelle Parteizugehörigkeit bei der Beantragung des Wohnberechtigungsscheines gespeichert worden sein, so kann er vom Recht auf Löschung Gebrauch machen. Diese Daten sind dann nämlich ohne jegliche Rechtsgrundlage gespeichert und müssen deshalb auf seinen Antrag hin gelöscht werden.

Anrufung des Berliner Beauftragter für Datenschutz und Informationsfreiheit (§ 27 BlnDSG)

Eines der wichtigsten Rechte ist das der Anrufung des Berliner Beauftragter für Datenschutz und Informationsfreiheit (§ 27 BlnDSG).

Sollten irgendwelche Probleme mit seinen gespeicherten Daten oder Unsicherheiten deswegen auftreten, so hat jeder das Recht, den Berliner Beauftragter für Datenschutz und Informationsfreiheit ohne irgendwelche vorgeschalteten Instanzen direkt anzurufen.

Der Berliner Beauftragter für Datenschutz und Informationsfreiheit kann den Betroffenen dann bei der Wahrnehmung seiner Rechte behilflich sein und seinerseits bei den Behörden nachfragen.

Recht auf Schadenersatz und Unterlassungsanspruch (§ 18 BlnDSG)

Ist einem ein Schaden durch die Verarbeitung personenbezogener Daten entstanden, hat man das Recht auf Schadenersatz und Unterlassungsanspruch (§ 18 BlnDSG) und zum Antrag auf Verfolgung einer Straftat (§ 32 Abs. 3 BlnDSG).

Sollte durch die Verarbeitung von Daten ein Vermögensschaden eingetreten sein, so steht dem Geschädigten Schadenersatz zu. Auch für einen Schaden, der nicht Vermögensschaden ist, steht ihm eine Entschädigung in Geld zu.

Das heißt, wenn durch rechtswidrig gespeicherte Daten (beispielsweise wird im Wohngeldantrag eine Zugehörigkeit zur KPD gespeichert und dieser Sachverhalt wird dem Arbeitgeber bekannt – weil dieser die Einkommensangaben bestätigen muss – und dem Wohngeldantragsteller daraufhin das Beschäftigungsverhältnis gekündigt wird), steht dem Betroffenen ein Schadenersatz für den erlittenen Vermögensschaden zu.

Der andere Fall wäre, wenn durch die Verbreitung der Information über eine AIDS-Krankheit alle Nachbarn nicht mehr mit dem Betroffenen sprechen und ihn meiden würden. In diesem Fall steht ihm auch ein finanzieller Schadenersatz zu.

Einen Antrag auf Verfolgung einer Straftat kann nur der Betroffene oder der Berliner Beauftragter für Datenschutz und Informationsfreiheit stellen. Die Tat wird nur auf Antrag verfolgt. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist auch gegen den Willen des Betroffenen zum Antrag berechtigt. Als Straftat gilt, wenn man unbefugt personenbezogene Daten, die nicht offenkundig sind, übermittelt, verändert, abruft oder sich aus verschlossenen Behältnissen verschafft. Dies kann mit Freiheitsstrafe bis zu einem Jahr oder mit einer Geldstrafe geahndet werden.

Nach den Kontrollmöglichkeiten durch den Betroffenen selbst, stehen noch zwei weitere Stufen zur Kontrolle bereit.

8.1.5.2. Eigenkontrolle

Hierbei kontrolliert sich die datenverarbeitende Behörde selbst, indem sie einen behördlichen Beauftragten für Datenschutz und Informationsfreiheit ernennt.

Dieser kontrolliert in der Behörde die Einhaltung des Datenschutzgesetzes. Er ist in dieser Funktion absolut weisungsfrei und direkt der Behördenleitung unterstellt. Allerdings hat er auch keinerlei Weisungsbefugnisse.
Er kann in seiner Funktion nur Feststellungen treffen und die datenverarbeitende Stelle auf einen Verstoß aufmerksam machen. Für Ver-

stöße gegen den Datenschutz ist er nicht haftbar zu machen, hierfür haftet immer die datenverarbeitende Stelle.

8.1.5.3. Fremdkontrolle

Die Kontrolle der Behörden wird in Berlin durch den Berliner Beauftragten für Datenschutz und Informationsfreiheit wahrgenommen. Auch für die private Wirtschaft übernimmt diese Kontrolle jetzt der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Hierbei wird nach dem Bundesdatenschutzgesetz gearbeitet.

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit: *§§ 21, 22 und 24 bis 29 BlnDSG*

- ist oberste Landesbehörde,
- ist in Ausübung seines Amtes nur dem Gesetz unterworfen,
- untersteht der Dienstaufsicht des Präsidenten des Abgeordnetenhauses
- seine Amtszeit beträgt 5 Jahre.
- wird vom Abgeordnetenhaus mit den Stimmen der Mehrheit gewählt,
- kontrolliert die Einhaltung des Datenschutzgesetzes bei den Behörden,
- kann Empfehlungen zur Verbesserung des Datenschutzes geben,
- berät Behörden in Fragen des Datenschutzes,
- kann bei Verstößen gegen den Datenschutz dies beanstanden und die Behörde zu einer Stellungnahme auffordern,
- kann von jedem angerufen werden,
- erstattet jährlich einen Bericht über seine Tätigkeit und
- die Behörden sind ihm gegenüber zur Unterstützung verpflichtet,
- ist Auskunft und Einsicht zu allen Fragen, die den Datenschutz betreffen, zu gewähren. Es ist ihm Zutritt in alle Diensträume zu gewähren.

Desweiteren zählen zu den Kontrollmöglichkeiten die Pflichten der Verarbeiter personenbezogener Daten. Die Behörden (Verarbeiter) haben die Rechte des Betroffenen und des Berliner Beauftragten für Datenschutz und Informationsfreiheit zu beachten.

Sie sind zur Durchführung der Datenschutzgesetze verpflichtet. Sie haben ein Dateien- und Geräteregister zu führen und daraus Meldungen an den Datenschutzbeauftragten zu erstatten. *§§ 5, 19 und 25 BlnDSG*

Die Behörden haben einen behördlichen Datenschutzbeauftragten zu bestellen und sind zur Durchführung von technisch-organisatorischen Maßnahmen verpflichtet.

8.1.6. Technisch-organisatorische Maßnahmen

Es gibt zehn technisch-organisatorische Maßnahmen zum Datenschutz. Im Folgenden werden diese Möglichkeiten aufgeführt.

8.1.6.1. Zugangskontrolle

§ 5 Abs. 3 Nr. 1 BlnDSG

Das Ziel ist, unbefugten Personen den Zugang zu Datenverarbeitungsanlagen zu verwehren.

Um dies sicherzustellen, können Schließsysteme (Schlüssel oder Chipkarten) eingebaut werden oder eine Kontrolle durch Pförtner oder Wachschutz erfolgen. In jedem Fall ist festzulegen, welche Personen zugangsberechtigt sind.

8.1.6.2. Datenträgerkontrolle

§ 5 Abs. 3 Nr. 2 BlnDSG

Hier ist das Ziel unbefugtes Lesen, Kopieren, Verändern und Entfernen von Datenträgern zu verhindern. Maßnahmen hierfür sind eine Datenträgerverwaltung (Inventarisierung) einschließlich Kennzeichnung der Datenträger. Weiterhin sind Taschenkontrollen am Ein- und Ausgang sowie der Verschluss von Räumen, in denen Datenträger aufbewahrt werden, Maßnahmen der Datenträgerkontrolle.

8.1.6.3. Speicherkontrolle

§ 5 Abs. 3 Nr. 3 BlnDSG

Es soll unbefugtes Speichern, Kenntnisnehmen, Verändern oder Löschen von Daten verhindert werden. Es soll also verhindert werden, dass Personen Daten eingeben, bereits eingegebene Daten lesen, verändern oder löschen. Davor schützt der Einsatz von Sicherheitssystemen mit Identitätsprüfung und Protokollierung (Passwort und Benutzerkennung) und die Festlegung von Rechten (Berechtigung) für die einzelnen Nutzer.

8.1.6.4. Benutzerkontrolle

§ 5 Abs. 3 Nr. 4 BlnDSG

Sie soll verhindern, dass Unbefugte die Datenverabeitungssysteme mit Hilfe von Datenübertragungseinrichtungen benutzen. Das verhindert den Einsatz technischer Schutzsysteme mit personenbezogener Authentifizierung und eine Zugangskontrolle. Das heißt, man muss sich bei verschiedenen Datenbereichen (Verzeichnis Wohnungsamt und Sozialamt) jeweils mit Benutzerkennung und Passwort anmelden.

8.1.6.5. Zugriffskontrolle

§ 5 Abs. 3 Nr. 5 BlnDSG

Hier soll sichergestellt werden, dass ausschließlich auf Daten, für die eine Zugriffsberechtigung vorliegt, zugegriffen werden kann.

Das lässt sich durch die Festlegung differenzierter, Passwort gesteuerter Zugriffsberechtigungen und eines Aktivitätsprotokolls erreichen. Das heißt, ein Sachbearbeiter des Personalamtes hat nur Zugriff auf das Verzeichnis Personalamt und dort nur auf die Mitarbeiterdaten seiner Buchstaben. Alle seine Aktionen im Netzwerk werden protokolliert und können im Verdachtsfall des Missbrauches ausgewertet werden.

8.1.6.6. Übermittlungskontrolle

Sie soll aufzeichnen, an welche Stellen welche Daten wann übermittelt worden sind. *§ 5 Abs. 3 Nr. 6 BlnDSG*

Hierbei ist wieder die Protokollierung ein Mittel. Weiterhin ist die Prüfung der Empfangsberechtigung und die Bestätigung des Empfängers als Kontrollmöglichkeit zu nennen.

8.1.6.7. Eingabekontrolle

Diese soll die Nachvollziehbarkeit der Eingaben gewährleisten und Veränderungen und Löschung von Daten verhindern. Die automatische Protokollierung ist wiederum eine Möglichkeit und zum anderen ist es das Signieren von Erfassungsbelegen. *§ 5 Abs. 3 Nr. 7 BlnDSG*

8.1.6.8. Auftragskontrolle

Hier soll sichergestellt werden, dass bei einer Auftragsdatenverarbeitung durch einen Dritten nur Daten nach den Weisungen des Auftraggebers verarbeitet werden. Dabei helfen eine klare vertragliche Festlegung und die Kontrolle der Vertragserfüllung. *§ 5 Abs. 3 Nr. 8 BlnDSG*

8.1.6.9. Transportkontrolle

Soll das unbefugte Lesen, Kopieren, Verändern und Löschen von Daten bei der Übertragung oder beim Transport verhindern. Maßnahmen hierfür sind das Verschlüsseln der Daten bei der Übertragung, Liefer- und Begleitscheine und verschließbare Behälter beim Transport. *§ 5 Abs. 3 Nr. 9 BlnDSG*

8.1.6.10. Organisationskontrolle

Beinhaltet die Gestaltung der innerbetrieblichen Organisation nach den Erfordernissen des Datenschutzes. Dies kann durch die Fixierung der Arbeitsabläufe (Dienstanweisungen) und die Vorsorge gegen Schadensereignisse (Risikoanalysen) erreicht werden. *§ 5 Abs. 3 Nr. 10 BlnDSG*

8.1.6.11. Geräteverzeichnisse

Als letzte Kontrollmöglichkeiten sollen noch das interne Dateienverzeichnis und das interne Geräteverzeichnis vorgestellt werden.

Beide Verzeichnisse sind von den datenverarbeitenden Stellen zu führen und regelmäßig dem Berliner Beauftragten für Datenschutz und Informationsfreiheit zu übermitteln. Für die automatisierte Verarbeitung hat die datenverarbeitende Stelle schriftlich folgendes festzulegen:

- Name und Anschrift der datenverarbeitenden Stelle, *§ 19 Abs. 2 BlnDSG*
- Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,
- Beschreibung der betroffenen Personengruppe und der diesbezüglichen Daten oder Datenkategorien,

- Empfänger oder Kategorien von Empfängern, denen die Daten übermittelt werden,
- Herkunft regelmäßig empfangener Daten,
- Zugriffsberechtigte Personen oder Personengruppen,
- Fristen für Sperrung und Löschung der Daten,
- Geplante Übermittlung personenbezogener Daten an Behörden…,
- Betriebsart des Verfahrens…,
- Beschreibung der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung,
- Ergebnisse der Vorabkontrolle.

8.2. Datensicherheit (IT-Sicherheit)

8.2.1. Definition

Die Datensicherheit ist ein wesentlicher Bestandteil der Informationstechnik und der Informationsverarbeitung.

Allgemein versteht man unter IT-Sicherheit (Datensicherheit) den Beitrag zur Sicherstellung der Verfügbarkeit und Integrität der Systeme, Programme und Daten sowie der Vertraulichkeit der Programme und Daten.

Hieraus ergeben sich als Folge dieser Definition die drei Grundbedrohungen der Sicherheit von informationsverarbeitenden Systemen, Programmen und Daten:

Bedrohung der **Verfügbarkeit**:

Die Verfügbarkeit eines technischen Systems ist die Wahrscheinlichkeit oder das Maß, dass das System bestimmte Anforderungen zu bzw. innerhalb eines vereinbarten Zeitrahmens erfüllt, und ist somit eine Eigenschaft des Systems.

Bedrohung der **Integrität**:

Integrität steht dafür, dass Daten über einen bestimmten Zeitraum vollständig und unverändert sind.

Bedrohung der **Vertraulichkeit**:

Unter Vertraulichkeit versteht man, dass eine Information nur für Befugte zugänglich ist, Unbefugte dagegen keinen Zugang zu der Information haben. Diese Bedrohungen können durch verschiedene Ursachen ausgelöst werden:

- Irrtümer,
- Nachlässigkeit,
- Benutzer- und Programmfehler,
- Technische Störungen,

- Systemausfall,
- Stromunterbrechung,
- Computerkriminalität (Viren) und Sabotage,
- Elementarschäden wie z. B. Feuer, Überschwemmung, Blitzschlag und Erdbeben.

Welche Auswirkungen ein Datenverlust haben kann und wie wichtig Gegenmaßnahmen sind, wird durch die Aussage von Sicherheitsexperten deutlich.

”Eine Firma, die komplett auf die Datenverarbeitung vertraut und die alle Daten unwiederbringlich verliert, ist innerhalb von 7 Tagen ruiniert und kann Konkurs anmelden. Selbst bei der Möglichkeit der Wiederherstellbarkeit der Daten entstehen der Firma derart hohe Kosten für die Wiederherstellung und den damit verbundenen Zeitaufwand, dass ein Überleben der Firma nicht zu erwarten ist.”

Diese Aussage ist allerdings nur dann zutreffend, wenn nichts für die Sicherung getan wurde.

8.2.2. Möglichkeiten der Sicherung

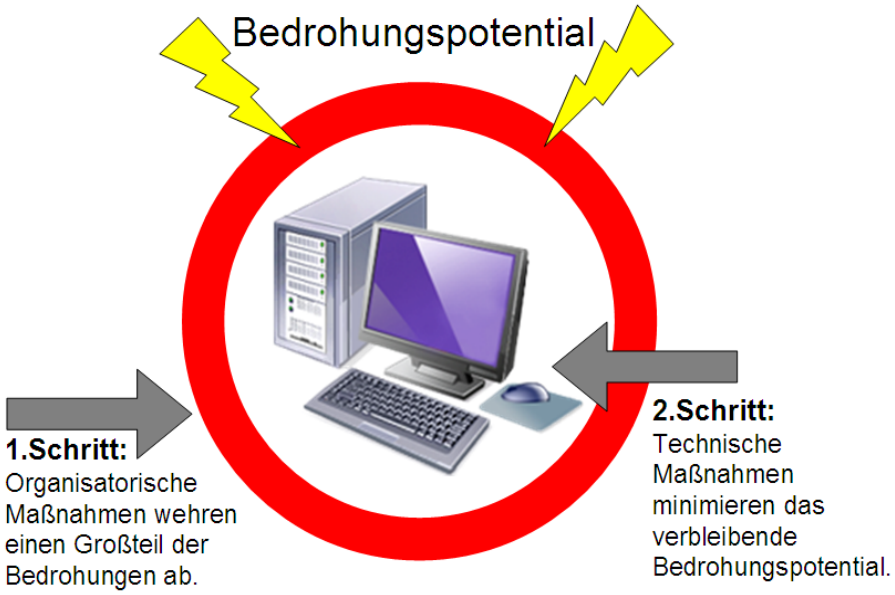
Ein mögliches Bedrohungspotential wird im ersten Schritt durch eine organisatorische Maßnahme abgewehrt. Hier ist die Rede von einer Bedrohungs- und Risikoanalyse.

Zu diesem Zweck werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) diverse Arbeitswerkzeuge bereitgestellt, wie z. B. die BSI-Standards zum Informationssicherheitsmanagement, die IT-Grundschutz-Kataloge, das GSTOOL und die ISO 27001-Zertifizierung auf Basis von IT-Grundschutz, die sowohl eine Prüfung des Informationssicherheitsmanagements als auch der konkreten Sicherheitsmaßnahmen auf Basis von IT-Grundschutz umfasst.

Bundesamt für Sicherheit in der Informationstechnik

Mit dem sogenannten GSTOOL stellt das BSI seit 1998 eine regelmäßig aktualisierte, innovative und ergonomisch handhabbare Software bereit, die den Anwender bei Erstellung, Verwaltung und Fortschreibung von IT-Sicherheitskonzepten entsprechend dem IT-Grundschutz effizient unterstützt.

In einem zweiten Schritt wird durch technische Maßnahmen das verbleibende Bedrohungspotential minimiert.



Eine vollkommene Sicherung ist nicht möglich, ein gewisses ”Restrisiko” bleibt immer übrig. Allerdings kann man dieses so gering wie möglich halten.

8.2.2.1. Organisatorische Maßnahmen

Es sollte eine Bedrohungs- und Risikoanalyse (s.o.) durchgeführt werden. In dieser Analyse sind mindestens folgende Punkte zu berücksichtigen:

- Wie wertvoll (wichtig) sind die Daten und auf welchen Rechnern sind sie gespeichert?
- Was wären die Konsequenzen aus einem Datenverlust?
- Könnten die Daten ersetzt oder wiederhergestellt werden?
- Wenn ja, welche Personalressourcen und Kosten (Zeit) sind damit verbunden?
- Wie kann ich Daten sichern, wie werden sie gesichert?
- Müssen ältere Datensätze aufgehoben werden?
- Wenn ja, auf welchem Medium und wie lange?
- Wie sicher sind Datenträger (Aktuell und Sicherung)?
- Wie können Mitarbeiter motiviert oder angewiesen werden, Sicherungsmaßnahmen regelmäßig durchzuführen?

Hiernach sind die erforderlichen Maßnahmen zu treffen. Es ist auf die Angemessenheit zu achten!!!

Als weiterer Schritt ist der Sicherheitsaufwand den Mitarbeitern und Systembetreuern zu verdeutlichen. Dies kann durch eine Arbeits- oder Dienstanweisung, in der die einzelnen Tätigkeiten und Verantwortlichkeiten geregelt sind und die eine Verfahrensbeschreibung enthält, erreicht werden.

Hier spielt auch die erste Aussage wieder eine Rolle, es sind ”nur” die erforderlichen Maßnahmen zu treffen. Denn wenn die Akzeptanz der Mitarbeiter für die Maßnahme fehlt, wird sie nicht durchgeführt (z. B. tägliche Datensicherung von reinen Textdateien auf Diskette und Aufbewahrungzeiten der Disketten von einem Jahr).

Gleichbedeutend ist die Sicherheitsmotivation. D.h. die Mitarbeiter und Systembetreuer müssen das Sicherheitsmanagement aktiv mittragen.

8.2.2.2. Technische Möglichkeiten

Die technischen Möglichkeiten entsprechen größtenteils den technisch-organisatorischen Maßnahmen zum Datenschutz.

Es sind die Zugangs-, Datenträger-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle. Weitere technische Möglichkeiten sind:

- keine Laufwerke in/an den Rechnern
- regelmäßige Festplatten- und Controllerspiegelung
- Serverspiegelung
- keine Einzelplatz-PCs
- Notstromversorgung
- Überspannungsschutz
- regelmäßige Datensicherung (auch auf externen Datenträgern)

8.2.2.3. Sicherungsstrategie

Es gibt verschiedene Sicherungsstrategien, nach denen man seine Daten sichern kann. Ein Beispiel ist das Sohn - Vater - Großvater - Prinzip:

Sohn - Vater - Großvater - Prinzip

Tagessicherung (Sohn) auf Datenträger T1 bis T4:

Montag	Dienstag	Mittwoch	Donnerstag
T1	T2	T3	T4

Freitag:Wochensicherung (Vater) auf Datenträger W1 bis W3:

1. Woche	2. Woche	3. Woche
W1	W2	W3

4. Woche: Monatssicherung (Großvater) auf Datenträger M1 bis M3:

Januar	Februar	März
M1	M2	M3

Entweder wird die Datensicherung dann archiviert oder es werden die Datenträger erneut verwendet und die alten Sicherungen überschrieben. Als Datenträger bieten sich hier Streamerbänder (Tapes) an. Aufgrund der zwischenzeitlich sehr umfangreichen Datenmengen scheidet die Diskette als Speichermedium aus.

Bei der Sicherung von Daten kann auch das IT-Dienstleistungszentrum Berlin behilflich sein. Dort werden zurzeit rund 44 Terrabyte (Stand: Mitte 2007) an Daten regelmäßig gesichert.

8.2.3. Unterscheidung Einzelplatz / Netz

Die Sicherheit einer Datenverarbeitungsanlage ist auch im wesentlichen von den verwendeten Rechnern und dem Betriebssystem abhängig.

So sind vernetzte Einzelplatzrechner ein geringeres Sicherheitsrisiko als ”reine” Workstations (Stand-Allone-PC).

Bei einem Einzelplatzrechner mit dem Betriebssystem MS-DOS gibt es keinen Schutzmechanismus beim Starten des Rechners. Das heißt, wenn man den Rechner anstellt, ist man sofort auf der Betriebssystemebene und kann von dort jede Datei aufrufen und benutzen. Dies war mit ein Grund, keine PC mehr mit dem Betriebssystem MS-DOS zu betreiben.

8.2.4. Leitsätze zur IT-Sicherheit

Jedes Sicherheitssystem ist nur so sicher wie seine schwächste Stelle.

Das bedeutet, man braucht keine Schließanlage zu installieren, wenn während des Publikumverkehrs die Türen doch offen bleiben müssen.

Sicherheitssoftware schützt nur in dem Umfang, in dem sie installiert wurde. Ein Paket Sicherheitssoftware im Schrank beruhigt vielleicht, schützt jedoch nicht. Und auch ein gutes Sicherheitskonzept nutzt nichts, wenn es nicht von den Mitarbeitern getragen wird.

Jedes Passwort verliert seinen Sinn, wenn (unbefugte) Personen es ausfindig gemacht haben oder kennen. Passworte sollten niemandem bekannt sein, außer einem selbst. Selbst Kollegen brauchen das Passwort nicht, auch nicht während der Vertretung. Benötigte Dateien können kopiert werden.

Achten Sie auf Hinweise für die Entschlüsselung des Passwortes (z. B. an der Wand das Poster mit der Aufschrift FLORIDA und das Passwort lautet ebenso).

Jedes Sicherheitssystem, das in Pausen oder nach Feierabend seine Funktion einstellt, ist unbrauchbar. Eine Zugangskontrolle, die nach Feierabend nicht mehr durchgeführt wird, ist sinnlos.

Merke:

- Benutze ein Passwort wie eine Zahnbürste:
- Benutze es täglich!
- Ändere es regelmäßig und
- teile es mit niemand anderem!

Ein recht sicheres Kennwort könnte sein: 0aJ/4 %(hGs$df"Y! (16 Zeichen). Die Problematik solcher Zufallszeichenfolgen ist jedoch, dass sie schwer zu merken sind und deshalb irgendwo notiert werden.

Eine leichter zu merkende Alternative ist ein einstudierter, zeichenweise veränderter Satz wie:

dIE bANANE*3 durch 1/4 nIKOTIN (32 Zeichen),

Wichtig ist hier das Einstreuen von genügend Zufallszeichen. Gut geeignet ist die Verwendung der Anfangsbuchstaben eines Satzes:

Hd7B %sd7Z

gebildet aus den fett hervorgehobenen Zeichen von „**H**inter **d**en **7** **B**ergen **% s**ind **d**ie **7 Z**werge“, mit eingestreutem Sonderzeichen.

Die Verwendung von Sonderzeichen kann einen Sicherheitsgewinn bringen, da ein Kennwort dadurch komplexer wird. Es ist aber davon abzuraten, sofern das Kennwort auch im Ausland verwendet werden muss, da nicht auf allen Tastaturen die gleichen Sonderzeichen vorhanden sind.

Filmzitate, berühmte Aussprüche, Aneinanderreihungen von einfachen Wörtern, Geburtsdaten, Geburtsnamen, Haustiernamen, etc. sind als Kennwörter zu vermeiden, da sie mittels des Wörterbuchangriffes oder durch einen informierten Angreifer leicht geknackt werden können.

Ungünstige Kennwörter:

Ungünstige Kennwörter

- Hierzu zählt man die leichtesten Kennwörter, also Wörter die einen Sinn ergeben. Einige Beispiele:
- 123456, passwort, God oder Gott
- Eigennamen (da diese häufig in Wörterbüchern zu finden sind, wird ein Wörterbuchangriff ermöglicht)
- Triviale Tastaturzeichenfolgen (1qay2wsx, asdf, qwert …)
- Vokale oder Selbstlaute (aeiou), Geburtsjahre, Geburtstage o.ä. (1985, 5.1.1987)

Generell sollte man Kennwörter verwenden, die keine eindeutige Folge haben. Hierbei können Programme helfen, die Kennwörter erstellen (siehe unten).

8.2.5. Viren

8.2.5.1. Definition

Ein Computervirus (lateinisch: virus für „Gift“, „Schleim“; im Singular „das Computervirus“, alltagssprachlich auch „der Computervirus“, Plural „die Computerviren“) ist ein sich selbst verbreitendes Computerprogramm (nichtautonomes Störprogramm), welches sich in andere Computerprogramme einschleust und sich damit reproduziert.

Die Klassifizierung als Virus bezieht sich hierbei auf die Verbreitungs- und Infektionsfunktion. Neben der Vervielfältigungseigenschaft besitzt ein Virus einen Effektteil, der in Abhängigkeit von einer Auslösebedingung aktiv wird.

Die Wirkung reicht von Gag-Effekten über subtile Datenverfälschung bis hin zur totalen Datenvernichtung.

Einmal gestartet, kann es vom Anwender nicht kontrollierbare Veränderungen am Status der Hardware (z. B. Netzwerkverbindungen), am Betriebssystem oder an der Software vornehmen (Schadfunktion). Computerviren können durch vom Ersteller gewünschte oder nicht gewünschte Funktionen die Computersicherheit beeinträchtigen und zählen zur Malware.

8.2.5.2. Entwicklung

Im Januar 1986 ist der erste Virus (Brainvirus) aufgetaucht.

Seitdem haben sich die Computerviren rasend vermehrt. 1990 waren allein in Deutschland 9 % aller Rechner mit Viren verseucht, dass sind 270.000 PCs. Im Jahre 1991 gab es schon mehr als 1.000 Viren, im Jahr 1992 waren es dann über 2.000 Viren und für das Jahr 1993 schätzt man, dass es schon über 6.000 Viren waren. Hiervon sind jedoch noch ein Großteil ”eingefroren” gewesen, das heißt sie sind noch nicht verbreitet worden.

Heute werden täglich mehrere Hundert neuer so genannter Virensignaturen programmiert und „verteilt“.

8.2.5.3. Virenarten

- *Bootvirus*
  Der Virustyp ist resident im Hauptspeicher. Er infiziert andere Disketten und die Festplatte. (Beispiele: Michelangelo- oder Stoned-Virus)

- *Datei- oder Programmvirus*
  Dieser Virus wird beim Starten des Programmes, in dem er sich befindet, aktiv und sucht nach weiteren Programmen, um diese zu infizieren. Nach Programmende ist der Virus nicht mehr aktiv. Allerdings kann er sich während seiner Aktivphase auf alle Programme kopieren! (Beispiel: Tequilla- oder AIDS II-Virus)

- *Trojanische Pferde*
  Dies sind autonome Programme, die eine dokumentierte Funktion vortäuschen und dabei eine Stör- oder Schadensfunktion ausführen (Beispiel: bei dem Befehl ”dir” wird statt der Auflistung der Dateien und Verzeichnisse die Festplatte formatiert).

- *Logische Bomben*
  Sie werden nur einmal aktiv. Dies passiert zu einem vom Programmierer festgelegten Ereignis. Sie haben eine bestimmte Stör- oder Schadensfunktion und vermehren sich nicht.

  (Beispiel: Der Systembetreuer wird entlassen und hinterlässt zur nächsten Lohnabrechnung für die Belegschaft einen Virus.)

- *Computerwürmer*
  Dies sind autonome Segmente, die sich selbständig über Computernetze ausbreiten. Computerwürmer kopieren sich selbst ohne eine Auslösebedingung. Die Verbreitung geschieht sehr schnell.

  Eine Schadensfunktion gibt es nicht. Es gibt nur die Störfunktion, die darin besteht, dass die Systemressourcen belastet und überlastet werden.

- *Makroviren*
  Ein Makrovirus ist ein Virus, der sich in Dokumentdateien von Office-Anwendungen versteckt. Der Virus wird aktiv, wenn ein infiziertes Dokument geladen wird. Verbreitet sind Makroviren in erster Linie für Microsoft WORD. Viren für andere Anwendungen sind möglich.

8.2.5.4. Verbreitung

Viren werden hauptsächlich über Disketten, CD-ROM und Mailboxen übertragen. Vielfach sind sie in Raubkopien von Spielen und Programmen enthalten. Dies geschieht zum Großteil ohne das Wissen der ”Spender” solcher Disketten. Auch der Download aus dem Internet bzw. der „einfache“ Besuch von Internetseiten kann die Verbreitung von Viren forcieren.

8.2.5.5. Antivirenprogramm

Ein Antivirenprogramm (auch Virenscanner oder Virenschutz genannt, Abkürzung: AV) ist eine Software, die bekannte Computerviren,

Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Der Echtzeitscanner (engl. on-access scanner, real-time protection, background guard u.a.), auch Zugriffsscanner oder residenter Scanner genannt, ist im Hintergrund als Systemdienst (Windows) bzw. Daemon (Unix) aktiv und scannt alle Dateien, Programme, den Arbeitsspeicher und evtl. den HTTP- wie den FTP-Verkehr.

Der manuelle Scanner (engl. on-demand scanner), auch als Dateiscanner bezeichnet, muss vom Benutzer von Hand gestartet werden (On-Demand). Findet ein Scanner dann schädliche Software, erscheint eine Warnung und in manchen Fällen Optionen zur Reinigung, Quarantäne oder Löschung der befallenen Dateien.

Als Online-Virenscanner werden Antivirusprogramme bezeichnet, die ihren Programmcode und die Viren-Muster über ein Netzwerk (online) laden. Sie arbeiten im Gegensatz zu fest installierten Virenscannern nur im On-Demand-Modus. Das heißt der persistente Schutz durch einen On-Access-Modus ist nicht gewährleistet. Deshalb eignen sich Online-Virenscanner zwar zum Reinigen, nicht aber zum präventiven Schutz eines Systems. Auch besteht die Gefahr, dass ein befallener Rechner über die Verbindung zum Internet ferngesteuert werden kann, selbst Spam versendet oder andere Rechner angreift, während er für den Scan online ist. Daher sollte man ein potenziell befallenes System nach Möglichkeit umgehend vom Netz trennen und mit einem Offline-Scanner untersuchen.

Software	Hersteller	Betriebssystem	deutschsprachig	kostenlos
AntiVir PersonalEdition Classic	Avira	Windows, Linux, BSD, Solaris	ja	ja
avast! Home Edition	Alwil Software	Windows, Linux	ja	ja
AVG Anti-Virus Free	AVG Technologies	Windows	nein	ja
BitDefender Free Edition	Softwin	Windows	nein	ja
Kaspersky Anti-Virus	Kaspersky Lab	Windows	ja	nein
McAfee VirusScan Plus	McAfee	Windows	ja	nein
Norton AntiVirus	Symantec	Windows	ja	nein

Die so genannte Auto-, Internet-, oder auch Live-Updatefunktion, mit der automatisch beim Hersteller aktuelle Virensignaturen herunter geladen werden, ist bei Virenscannern von besonderer Bedeutung.

Wenn sie aktiviert ist, wird der Benutzer regelmäßig daran erinnert, nach aktuellen Updates zu suchen, bzw. die Software sucht selbstständig danach.

Es empfiehlt sich diese Option zu nutzen, um sicher zu gehen, dass das Programm wirklich auf dem aktuellen Stand ist. Die Häufigkeit mit der Updates von den Herstellern bereitgestellt werden, sagt jedoch nichts direkt über die Qualität des Produktes aus. Wichtiger ist, dass bei einer bestehenden Bedrohung möglichst zeitnah eine entsprechende Signatur veröffentlicht wird (Reaktionszeit).

Merke:

Das „beste“ Antivirenprogramm hat keine Wirkung, wenn nicht regelmäßige Signaturupdates in das Programm eingespielt werden.

8.2.5.6. Beseitigung

Bekannte Viren lassen sich meist durch die oben genannten Anti-Viren-Programme entfernen. Teilweise werden von einigen Herstellern spezielle Entfernungstools bereitgestellt, die jeweils nur für einen bestimmten Virus helfen.

Funktioniert dies nicht, so bleibt noch die Möglichkeit der Formatierung der Festplatte. Hierbei verliert man allerdings alle Daten.

8.2.6. Phishing

Phishing werden Versuche genannt, über gefälschte WWW-Adressen Daten eines Internet-Benutzers zu erlangen. Der Begriff ist ein englisches Wortspiel, das sich an fishing („Angeln“, „Fischen“) anlehnt. Evtl. in Anlehnung an Phreaking auch password fishing, bildlich das „Angeln nach Passwörtern mit Ködern“. Häufig wird das „h“ in dem Begriff mit harvesting erklärt, so dass der Begriff Phishing dann Password harvesting fishing lautet.

Phisher geben sich als vertrauenswürdige Personen aus und versuchen, durch gefälschte elektronische Nachrichten an sensible Daten wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen zu gelangen.

Phishing-Nachrichten werden meist per E-Mail oder Instant Messaging versandt und fordern den Empfänger auf, auf einer präparierten Webseite oder am Telefon geheime Zugangsdaten (meistens die Bankleitzahl in Verbindung mit der Kontonummer, PIN und TAN´s) preiszugeben.

Versuche, der wachsenden Anzahl an Phishing-Versuchen Herr zu werden, setzen unter anderem auf geänderte Rechtsprechung, Anwendertraining und technische Hilfsmittel.

Auch für Microsoft Outlook gibt es eine Möglichkeit, sich vor gefährlichem Phishing zu schützen. Dabei wird eine Symbolleiste in Outlook eingebunden, und jede eingehende E-Mail kann auf gefährliche Verweise und verdächtige Header hin überprüft werden. Das Programm Delphish ist dabei kostenlos verfügbar und versetzt den Nutzer entweder in die Lage, eigenständig eine Entscheidung über ein mögliches Phishing zu treffen, oder es stuft die E-Mail automatisch als Phishing ein. Bei der automatischen Einstufung wird auf eine Datenbank mit Phishing-E-Mails zurückgegriffen, oder es werden die Verweise in der E-Mail auf verdächtige Merkmale hin überprüft.

Vor einiger Zeit wurde bereits eine Spam-E-Mail mit folgendem Wortlaut verschickt:

> Sehr geehrter Kunde!
>
> Wir sind erfreut, Ihnen mitzuteilen, dass Internet – Ueberweisungen ueber unsere Bank noch sicherer geworden sind!
>
> Leider wurde von uns in der letzten Zeit, trotz der Anwendung von den TAN-Codes, eine ganze Reihe der Mitteldiebstaehle von den Konten unserer Kunden durch den Internetzugriff festgestellt.
>
> Zur Zeit kennen wir die Methodik nicht, die die Missetaeter für die Entwendung der Angaben aus den TAN – Tabellen verwenden. Um die Missetaeter zu ermitteln und die Geldmittel von unseren Kunden unversehrt zu erhalten, haben wir entschieden, aus den TAN – Tabellen von unseren Kunden zwei aufeinanderfolgenden Codes zu entfernen.
>
> Dafuer muessen Sie unsere Seite besuchen, wo Ihnen angeboten wird, eine spezielle Form auszufuellen. In dieser Form werden Sie ZWEI FOLGENDE TAN – CODEs, DIE SIE NOCH NICHT VERWENDET HABEN, EINTASTEN.
>
> Achtung! Verwenden Sie diese zwei Codes in der Zukunft nicht mehr!
>
> Wenn bei der Mittelueberweisung von Ihrem Konto gerade diese TAN – Codes verwendet werden, so wird es fuer uns bedeuten, dass von Ihrem Konto eine nicht genehmigte Transitaktion ablaeuft und Ihr Konto wird unverzueglich bis zur Klaerung der Zahlungsumstaende gesperrt.
>
> Diese Massnahme dient Ihnen und Ihrem Geld zum Schutze! Wir bitten um Entschuldigung, wenn wir Ihnen die Unannehmlichkeiten bereitet haben.
>
> Mit freundlichen Gruessen,
>
> Bankverwaltung

Sie forderte den Empfänger auf, einem Verweis zu folgen, der angeblich auf die Seiten der Postbank führen sollte, tatsächlich aber auf eine Phishingseite verwies. Diese fragte in fehlerhaftem Deutsch nach der PIN sowie zwei TANs. Nach Eingabe der Ziffern in die Formularfelder wurden die Eingabedaten zum Abruf durch den Betrüger abgespeichert. Der Besucher wurde an die öffentliche Postbank-Webadresse weitergeleitet.

8.2.7. Spam

Als Spam oder Junk (englisch für: „Abfall“ oder „Plunder“) werden unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten bezeichnet, welche dem Empfänger unverlangt zugestellt

werden und massenhaft versandt wurden oder werbenden Inhalt haben.

Spam verursacht im System der weltweiten Kommunikation erheblichen Schaden. Dieser ist vor allem auf die zusätzliche Datenmenge und den Aufwand der damit verbundenen überflüssigen Bearbeitung zurückzuführen.

8.2.8. Falschmeldungen

Die weitaus größte Gruppe unter den im Internet verbreiteten Falschmeldungen sind die Urban Legends (Großstadtmärchen, Wandersagen, Gerüchte). Hier wird auch der größte (und z.T. der amüsanteste) Unfug verzapft. "Die Spinne in der Yucca-Palme" ist der Titel eines Buch-Klassikers (ISBN 3-406-45995-1), der sich mit solchen Geschichten befasst.

Die Bandbreite der weiter erzählten Geschichten reicht von Gesundheitswarnungen aller Art (z. B. vor bestimmten, angeblich krebserregenden Lebensmitteln oder Kosmetika) über Warnungen vor bestimmten Tricks von Betrügern (die es in der Praxis nicht gibt) bis zu Horror-Geschichten darüber, was der Nichte des Friseurs des Bekannten einer entfernten Verwandten aus Dingsda "selber passiert" sein soll... Wichtige und recht aktuelle Informationen erhalten Sie auf der Webseite

http://www2.tu-berlin.de/www/software/hoax.shtml

Fragen zur Selbstkontrolle:

40. Welchen Sinn und Zweck soll der Datenschutz erfüllen?

41. Auf welchem Prinzip baut der Datenschutz auf?

42. Welche Kontrollmöglichkeiten bestehen?

43. Welche Bedrohung gibt es für Ihre Daten?

44. Welche Möglichkeiten der Sicherung gibt es?

45. Was sind Viren?

9. New Public Management

Lernziele:

Der /Die Lernende soll

- die Beziehungen des E-Government wiedergeben können,
- eine Auswahl der im Land Berlin vorhandenen E-Government-Projekte aufzählen können,
- die unterschiedlichen Formen der elektronischen Signatur beschreiben können,
- die Inhalte und Ziele des New Public Management wiedergeben können,
- die Elemente des Neuen Steuerungsmodell nennen können,

9.1. Inhalt und Ziele

Das New Public Management (NPM) oder auch Öffentliche Reformverwaltung bezeichnet eine Richtung innerhalb der Verwaltungsreform und Staatsmodernisierung, die auf der Übernahme privatwirtschaftlicher Managementtechniken beruht. Die Eckpunkte des New Public Management variieren je nach Land und/oder Autor.

In Europa fand vor allem in Großbritannien eine besonders radikale Variante des NPM Anwendung. NPM ist weitgehend eine Reaktion auf die „Finanzierungskrise des veralteten Wohlfahrtsstaates“ und entstammt den 1980er Jahren mit ihrer Dominanz wirtschaftsliberaler Regierungen, aber auch sozialdemokratischer Regierungen in Neuseeland oder Schweden.

Ziel ist eine effizientere Verwaltung durch Einführung betriebswirtschaftlicher Effizienzkriterien.

Gekennzeichnet ist das NPM durch Schlagworte wie Projektmanagement, flache Hierarchien, Kundenorientierung, Zielvereinbarungen, Umbau des Beamtenstatus, Entpolitisierung der Verwaltung und durch englische Ausdrücke wie lean management (schlankes Management), Total-Quality-Management (umfassendes Qualitätsmanagement), Benchmarking (setzen von Maßstäben) und Contracting-Out (Überlassung/Übertragung von als grundsätzlich öffentliche Aufgaben anerkannte Tätigkeiten an Organisationen in frei-gemeinnütziger oder privat-gewerblicher Trägerschaft (Non-Profit-Sektor)).

Kernelemente des NPM sind

- Neudefinition der Rolle und Funktionen durch stärkere Marktorientierung
- Verselbstständigung von Verwaltungseinheiten

- Reorganisation der Betriebsorganisation
- Modernisierung des Rechnungswesens und Einführung von Controllingkonzepten zur Ergebnissteuerung
- stärkere Kundenorientierung
- stärkere Leistungsorientierung in der Personalpolitik

9.2. Theoretisch-konzeptioneller Hintergrund

Es ist umstritten, ob das New Public Management ein kohärenter[11] und konsistenter[12] Ansatz ist.

Aufgrund der willkürlichen Zusammenstellung der einzelnen Bestandteile wie auch der unterschiedlichen theoretischen Strömungen, aus denen das New Public Management entstanden ist, kann ein universaler, naturgemäßer Kern nicht bestimmt werden.

Wesentliche theoretisch-konzeptionelle Grundströmungen im NPM sind Entscheidungsprozessansätze und Strukturen, die im Wesentlichen mehr Wahlrechte für die als Kunden der öffentlichen Verwaltung verstandenen Bürger einfordern und verschiedene Theorien und Ansätze mittlerer Reichweite wie etwa der Transaktionskostenansatz[13], Principal-Agent[14]-Ansätze (die im Wesentlichen die Trennung zwischen Auftraggeber und Auftragnehmer in der öffentlichen Produktion einfordern), aber auch verschiedene Qualitätsansätze in national sehr unterschiedlicher Gewichtung.

Daneben darf nicht übersehen werden, dass einige Staaten auch Qualität eng in Zusammenhang mit Nutzerdemokratie stellen, also die Mitbestimmung und Koproduktion der Empfänger von öffentlichen Leistungen an der Leistungsproduktion selbst (beispielsweise die Volksabstimmungen in der Schweiz).

Vor allem Neuseeland, die Niederlande und später Skandinavien dienten als Ideenlieferanten für die Ausarbeitung einer Schweizer Version des NPM: die wirkungsorientierte Verwaltungsführung.

Die ersten Reformbestrebungen gingen ungefähr im Jahr 1991 vorrangig von Chefbeamten in der Schweiz aus, die den als bürokratisch empfundenen Staat wieder handlungsfähiger machen wollten.

1993 wurden dort erste größere Projekte gestartet, die ca. drei Jahre später mit sogenannten Pilotämtern getestet wurden.

Ungefähr seit dem Jahr 2000 erfolgte die definitive Umsetzung in den meisten Kantonen, jedoch noch wenigen Städten. Auch auf Bundesebene findet die wirkungsorientierte Verwaltungsführung nur zurückhaltend statt.

---

11 zusammenhängender, einheitlicher

12 in Zusammenhang stehender

13 Unter Transaktionskosten sind Kosten zu verstehen, die im Zusammenhang mit der Nutzung einer Sache entstehen, z.B. die Kosten einer Überweisung bei der Mietzahlung.

14 bietet ein Modell, um das Handeln von Menschen in einer Hierarchie zu erklären

Was die Schweiz von anderen Ländern unterscheidet, ist der starke und konsequente Bezug zur Wirkung staatlichen Handelns. Zwar ist auch hier die Wirkungsmessung ein weitgehend ungelöstes Problem, doch die Grundhaltung der Ausrichtung aller Maßnahmen an Wirkungszielen ist unbestritten.
Außerdem erlaubt das politische System der Schweiz ein ausgesprochen pragmatisches, lösungsorientiertes Vorgehen.
In Deutschland ist die Gesamtheit der Vorgänge des Wahrnehmens der internationalen Ansätze zur Modernisierung des Staates auf kommunaler Ebene selektiv ausgerichtet. Das deutsche Neue Steuerungsmodell in seiner Originalfassung von 1993 weist einige wesentliche Unterschiede zu anderen nationalen Modernisierungsprogrammen auf.
Gleichwohl lässt sich das Neue Steuerungsmodell auch als eine Variante des New Public Management bestimmen.

9.3. Kritik

Dominant ist die Kritik, NPM sei „staatsfeindlich“, fordere den „Rückbau des Staates“, begünstige einseitig private Erstellung und Erfüllung von Aufgaben („Privatisierung“) und zerstöre die Grundlagen der mitwirkenden Demokratie, da die Reduktion des Bürgers zum schlichten Kunden keinen Fort-, sondern einen undemokratischen Rückschritt darstelle (Wilson).

Von der besonders aus dem akademischen Bereich kommenden Kritik wird dem NPM vorgeworfen, von einer zu großen Ähnlichkeit von Staat und privatem Sektor auszugehen, obwohl den Staat sein Gewaltmonopol kennzeichnet und sich staatliches Handeln am Gemeinwohl zu orientieren hat; die Geschäftswelt kennzeichnet demgegenüber ein Streben nach Gewinnmaximierung.

Besonders wichtig ist die Kritik von betriebswirtschaftlicher Seite, dass NPM überhaupt keine Effizienzverbesserung herstellt, da unter anderem mit Pseudo-Märkten agiert werde, dass die Reformen teurer seien als jede Einsparung und dass NPM-Strukturen der Aufgaben gerade hinsichtlich der Wirtschaft nicht gewachsen sind.

9.4. Neues Steuerungsmodell

9.4.1. Begriff und Inhalte

Neues Steuerungsmodell (NSM)

Der Begriff *Neues Steuerungsmodell (NSM)* bezeichnet in der Organisationslehre öffentlicher Verwaltungen ein Modell zur strategischen Steuerung von Verwaltungen, insbesondere im kommunalen Bereich.
In Ergänzung dazu beschreibt die Doppik die finanzwirtschaftlichen Instrumente und Verfahren, die dem zukünftigen Einsatz der doppelten Buchführung in den öffentlichen Verwaltungen dienen.

Beiden Modellen ist gleich, dass eine Steuerung der Leistungserstellung öffentlicher Verwaltungen über die Produkte13 stattfindet, die sich am Markt ausrichten.

9.4.2. Ausgangssituation und Geschichte

Die Steuerung der öffentlichen Verwaltung richtete sich schon von jeher an der Erfüllung öffentlicher Aufgaben aus. Ergänzt wurde diese Ausrichtung durch eine überwiegend juristisch orientierte Sichtweise der Aufgabenerledigung.

Grundlage des Verwaltungshandelns in Kommunalverwaltungen war so u.a. der Aufgabengliederungsplan der KGSt (Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung, ab November 2005 Kommunale Gemeinschaftsstelle für Verwaltungsmanagement).

Diese Sichtweise vernachlässigte aber jegliche betriebswirtschaftlichen Instrumente, sowohl im Führungs- als auch im Finanzmanagement. Dies führte zu finanziellen Problemen, da der echte Ressourcenverbrauch nicht gemessen wurde und die Steuerung der Verwaltungen sich auf juristische Aspekte beschränkte.

Ende der 80er Jahre summierten sich die daraus resultierenden Probleme aufgrund folgender Ursachen:

- Die Finanzprobleme öffentlicher Verwaltungen wurden aufgrund geänderter wirtschaftlicher Rahmenbedingungen zu strukturellen Problemen.
- Die Bürger drängten immer mehr auf Kundenorientierung.
- Die Kosten der Deutschen Einheit verstärkten die finanziellen Probleme öffentlicher Verwaltungen deutlich.
- Den Verwaltungen wurde zunehmend ökologisches und ökonomisches Handeln abverlangt.

Das Neue Steuerungsmodell entspricht in weiten Teilen, insbesondere was die Binnenorganisation betrifft, dem internationalen Trend des New Public Management. Gegenüber dem im internationalen Bereich propagierten New Public Management wurde das Neue Steuerungsmodell allerdings auf der Kommunalen Ebene entwickelt.

Das NSM empfiehlt: Eine Steuerung der Organisationseinheiten nicht über die Zuweisung von Haushaltsmitteln („.. es gibt x Millonen Euro für das Personal des Stadttheaters..“), sondern über die (zusätzliche) Definition des erwarteten Outputs (Beispiel: „...mit den zugewiesenen Haushaltsmitteln wird das Theater im kommenden Haushaltsjahr x Vorstellungen mit y Zuschauern und einer durchschnittlichen Steigerung der Sitzplatzauslastung um z % anbieten..“).

Outputorientierung

Das Stichwort dazu hieß *Outputorientierung*. Gleichzeitig sollen die dezentralen Organisationseinheiten die zur Erstellung des Outputs (= der Produkte) erforderlichen Ressourcen nicht mehr einzeln zugewiesen bekommen (= eine Schule sollte die Lampe für den Tageslicht-

projektor nicht mehr einzeln beim Schulverwaltungsrat beantragen etc.), sondern die Organisationseinheiten sollen mehr **dezentrale Ressourcenverantwortung** durch eigene Budgets erhalten.

Damit sie diese Mittel nicht sachfremd einsetzen, muss der Output entsprechend definiert und die Einhaltung solcher Vereinbarungen im Rahmen von „Kontraktmanagement“ gesichert werden. Zusätzlich zu den drei hier genannten Elementen des NSM ist „Wettbewerb“ das vierte Element des NSM.

Von Beginn an wurde betont, dass eine betriebswirtschaftliche Steuerung im öffentlichen Bereich mit der veralteten Kameralistik, die allein den „Geldverbrauch“ misst und den „Ressourcenverbrauch“ nicht kennt, stets unvollständig bleiben wird.

Damit ist es möglich, dass für Ausgaben in der Zukunft keine oder nicht ausreichende Rücklagen geschaffen wurden, zum Beispiel für die Pensionszahlungen der Dienstkräfte, die sich in einem öffentlichen Dienst- und Treueverhältnis befinden (Beamte).

Um die Kameralistik abzuschaffen und durch ein neues, an die Privatwirtschaft angelehntes Rechnungswesen zu ersetzen, mussten zunächst Gesetze geändert werden. Im November 2003 beschloss die Innenministerkonferenz, in den Kommunen wahlweise ein doppisches Rechnungswesen oder eine sog. erweiterte Kameralistik einzuführen.

In der Folge dieses Beschlusses haben alle Länder ihre Gemeindeordnungen und Gemeindehaushaltsverordnungen entsprechend geändert. Für das Haushalts- und Rechnungswesen des Bundes und der Länder wurde das Haushaltsgrundsätzegesetz im Jahr 2009 so verändert, dass die Doppik angewandt werden konnte.

Die Länder Hamburg und Hessen waren die ersten, die ihr Haushalts- und Rechnungswesen entsprechend umgestellt haben. Berlin arbeitet noch immer mit dem kameralen Haushaltswesen…

9.4.3. Erläuterung der Elemente

Das Neue Steuerungsmodell besteht im Wesentlichen aus folgenden Elementen:

Strategische Steuerung der Verwaltung durch Politik und Verwaltungsführung

Bisher wurde die Verwaltung durch den Gemeinderat und die Verwaltungsspitze aufgrund von Einzelfallentscheidungen gesteuert. Im NSM sollen nun Zielvereinbarungen zwischen den Ämtern/ Fachbereichen und der Führung vereinbart werden, so genanntes Kontraktmanagement. Um dieses Ziel erreichen zu können, wird dem Fachbereich ein Budget zur Verfügung gestellt. Die Zielerreichung wird am Ende des Haushaltsjahres überprüft.

Einführung moderner Instrumente des Personalmanagements

Mit diesem Element sollte eine zunehmende Delegation von Verantwortung und zusätzliche Qualifizierung des Personals erfolgen. Führungskräfte werden nicht mehr nach Zugehörigkeit oder Dienstalter ausgesucht, sondern nach Führungsqualifikation (Assessmentcenter). Zusätzlich werden diese Führungskräfte auf entsprechende Seminare geschickt, um ihnen das erforderliche Wissen beizubringen

Budgetierung

In Abkehr zu der vorherigen, einzelfallorientierten Zuteilung von Mitteln durch die zentrale Finanzverwaltung (Kämmerei o.ä.) soll im Neuen Steuerungsmodell jedem Fachbereich ein eigenes Budget zugeteilt werden. Die Verwendung des Budgets muss nicht mehr für jeden Fall vorher genehmigt werden, sondern kann eigenverantwortlich erfolgen. Wichtig dabei ist aber das Erreichen der vorher vereinbarten Ziele.

Dezentrale Ressourcenverantwortung

Eng verbunden mit der Budgetierung ist die Verantwortung für die Ressourcen durch den Fachbereich. Im alten Modell teilten Personalamt, Hauptamt 14und Kämmerei die Ressourcen Personal, Material und Finanzen dem jeweiligen Fachbereich zu. Dies bedeutete, dass Amtsleiter ihr Personal nicht selbst aussuchen konnten und um Mittel kämpfen mussten. Im NSM wird Ihnen das Recht, die Ressourcen selbst zu bewirtschaften, zugestanden. Dies führt häufig zu einer deutlichen Effizienzsteigerung und Senkung der Kosten.

Outputorientierte Steuerung auf der Grundlage von Produktbeschreibungen

Bisher stand im Fokus der Verwaltung die rein juristisch orientierte Aufgabenerledigung, von der dann in aller Regel behauptet wurde, dass sie nicht wirtschaftlich erledigt werden könne.

Das NSM stellt das Produkt in den Vordergrund, dessen optimale Erbringung sich nicht nur am Gesetz, sondern vor allem an den damit verbundenen Kosten und an der Erfüllung der Erwartungen des Bürgers orientiert.

Um diese Produkte erbringen zu können, ist natürlich deren vorherige Definition erforderlich. Der Produktkatalog ersetzt insofern den Aufgabengliederungsplan.

Berichtswesen und Controlling

Wie beim Element der „Strategischen Steuerung“ beschrieben, werden zwischen der Verwaltungsführung und den Fachbereichen Zielvereinbarungen geschlossen. Um den Grad der Zielerfüllung zu messen und um auch im laufenden Haushaltsjahr auf gravierende

Abweichungen steuernd eingreifen zu können, wird ein Berichtswesen eingeführt.
Dieses Berichtswesen liefert in periodischen Abständen (Monate, Quartale) eine Übersicht über die Entwicklung vorher festgelegter Kennzahlen an die Entscheidungsträger (Ausschüsse, Bürgermeister usw.).

Parallel dazu wird durch strategisches und operatives Controlling eine unterstützende Ebene durch die Verwaltung selber eingebaut.

Technikunterstützte Informationsverarbeitung

Integrierte Systeme, die Information auf verschiedensten Ebenen anbieten und auch Frühwarnfunktionen besitzen, werden zunehmend angestrebt. Insellösungen mit Hilfe von Standardsoftware („Eigenprogrammierungen“ mit Excel oder Access) werden nach und nach abgelöst.

Wettbewerb zur Erhöhung von Wirtschaftlichkeit, Produkt- und Dienstleistungsqualität

Um einen „Innovationsdruck“ zu erzeugen, wird im NSM echter Marktwettbewerb oder – wo dies nicht geht, also bei hoheitlichen Aufgaben – künstlicher Wettbewerb eingeführt.

Bei diesem künstlichen Wettbewerb handelt es sich vor allem um Kennzahlenvergleiche: Verwaltungen vergleichen anhand vorher festgelegter Kennzahlen die erbrachten Leistungen, was die teuer produzierenden Bezirke dazu zwingt, ihre Leistungserstellung zu überdenken.

Neben den interkommunalen Vergleichen sind auch echte Vergleiche mit dem Markt vorhanden, wie z.B. beim kommunalen Gebäudemanagement.

9.4.4. Bewertung

Das neue Steuerungsmodell hat Anfang der 90er Jahre grundsätzlich den Ansatz eines praktikablen und zukunftsweisenden Modells gehabt. Der ganzheitliche Ansatz dieses Modells hat sich jedoch nie richtig durchsetzen können. Dies liegt zum einen sicher an der Unverbindlichkeit, da es nie als Verpflichtung in Form eines Gesetzes o.ä. erlassen wurde. Viele Kommunen haben jedoch einzelne Elemente eingesetzt oder auf dem NSM aufbauend umfassende Reformen eingeleitet, die im Endeffekt aber nur zu rudimentären Verbesserungen führten.

Das größte Problem des Neuen Steuerungsmodells war aber seine einseitige Orientierung an der inneren Organisation. Dies führte dazu, dass finanzwirtschaftliche Instrumente nur sehr vage oder gar nicht im NSM enthalten sind.

Deutlich wird dies an der Budgetierung, die zwar als unverzichtbares Element von der KGSt beschrieben wird, aber in vielen örtlichen Reformprojekten nicht konsequent umgesetzt wurde.

Die Kommunen fokussierten auf Produktdefinition, um den Output besser steuern zu können. Dabei fehlte zum einen die Verknüpfung zum (nach wie vor) wichtigsten Steuerungsinstrument, dem kommunalen Haushalt.

Und zum anderen wurden Leistungen nur vage definiert:

- Was beispielsweise ist genau die Leistung einer Schule?

Und vor allem:

- Wie kann man die Qualität messen?

Viele hoheitliche Aufgaben lassen keine Budgetierung zu, weil sich die Ausgaben meist nicht vorhersagen lassen (Sozialleistungen), bzw. Einnahmeerwartungen (Steuern) nicht erfüllt werden können.

Inzwischen wurde mit dem Beschluss der Innenministerkonferenz vom November 2003 der Weg für ein neues Gemeindehaushaltsrecht frei gemacht.

10. E-Government

Unter E-Government (deutsch: Regieren und Verwalten mit Informations- und Kommunikationstechnologien über elektronische Medien, aber auch: E-Regierung, elektronische Regierung) im weiteren Sinn versteht man die Vereinfachung und Durchführung von Prozessen zur Information, Kommunikation und Transaktion innerhalb und zwischen staatlichen Institutionen sowie zwischen diesen Institutionen und Bürgern bzw. Unternehmen durch den Einsatz von Informations- und Kommunikationstechnologien.

Mit eGovernment erscheint nun ein neues Reformkonzept, das sich anschickt, New Publik Management als das Schlagwort der Verwaltungsmodernisierung abzulösen. Inwieweit kann nun eGovernment in diesen Kontext der Verwaltungsmodernisierung eingebunden werden?

Hierzu gibt es zwei unterschiedlich Sichtweisen:

a) Zum einen die Institutionensicht, bei der die Auswahl und das Design institutioneller Rahmenbedingungen für die neuen Prozessmodelle“ (Schuppan/Reichard 2002b: 40-41) betrachtet werden. Diese Sicht wird im Folgenden nicht weiter betrachtet.
b) Zum anderen aus der Sicht der Gestaltung neuer öffentlichen Leistungsketten bzw. deren Optimierung mit den Möglichkeiten, die die IuK-Technik bietet (Prozesssicht).

Erst diese eröffnet in vielen Bereichen die zusätzlichen Möglichkeiten um die Leistungsfähigkeit und Effizienz öffentlicher Institutionen zu verbessern, das Leistungsangebot zu erweitern und das Ganze auch noch mit mehr Kundenorientierung zu gestalten.

effizient – sicher – vernetzt
e-government 2.0

Ausgehend vom Aktionsplan E-Government der europäischen Initiative i2010, den Erfahrungen mit BundOnline 2005 und Deutschland-Online hat die Bundesregierung am 13. September 2006 das Programm E-Government 2.0 als Konkretisierung eines Teils der Gesamtstrategie im Regierungsprogramm „Zukunftsorientierte Verwaltung durch Innovation“ beschlossen.

Die Umsetzung des Programmes erfolgt durch alle Bundesressorts, die Koordinierung findet im Bundesministerium des Innern. E-Government wird damit zur Daueraufgabe der Verwaltungsmodernisierung. Gleichzeitig ist der Staat mit E-Government Nachfrager und Förderer von Zukunftstechnologien und sichert die erforderlichen Infrastrukturen der Informationstechnik.

Das Internet soll damit zum bevorzugten Kommunikations- und Vertriebskanal für bedarfsgerechte Verwaltungsdienstleistungen werden. Die größten Effizienzpotenziale gilt es an der Schnittstelle zwischen Wirtschaft und Verwaltung durch die elektronische Verknüpfung ihrer Prozessketten zu erschließen.

Zur E-Government-Entwicklung in der Berliner Verwaltung liegt ein umfassender Plan für den Weg in die Informationsgesellschaft vor, der "Masterplan E-Government". Die wichtigsten Ziele auf diesem Weg sind:

- Bürger und Wirtschaft sollen mit Hilfe der Informationstechnik umfassend und aktuell über alle Dienstleistungen der Verwaltung informiert werden. Formulare, Anträge, Vorschriften und Gesetzestexte sollen rasch und ohne Aufwand zugänglich sein.
- Der Zugang zur Verwaltung und zu ihren Dienstleistungen soll erleichtert werden. Computer und Telefon sollen helfen, ohne Umwege den richtigen Ansprechpartner und die richtige Behörde zu erreichen. Das Bürgerbüro und eine Anlaufstelle für Unternehmen müssen die bisherigen Behördengänge ablösen.
- Innerhalb der Verwaltung soll die Informationstechnik genutzt werden, um die gewünschten Dienstleistungen schneller und mit weniger Aufwand bereitzustellen.

Im Vordergrund stehen dabei nicht die vielen einzelnen Verwaltungsverfahren, auf die sich die Veränderungswünsche richten. Es sollen zunächst die organisatorischen, technischen und rechtlichen Voraussetzungen und Rahmenbedingungen geschaffen werden, um dann allerdings ein rasches Wachstum und eine vielfältige Nutzung der neuen Möglichkeiten zu eröffnen.

In Berlin werden alle Aktivitäten im IT-Kompetenzzentrum der für Inneres zuständigen Senatsverwaltung koordiniert.

An der Ausgestaltung des Masterplans zur Entwicklung des E-Government der Berliner Verwaltung mit dem Titel "Ziele, Strategie und Handlungsfelder einer interaktiven Verwaltung" wirkten alle Senatsressorts und Bezirke Berlins mit. Um die definierten Ziele des Masterplans in Berlin effizient umzusetzen, wurde als Strategie ein 8-Punkte-Programm vorgeschlagen.

Mit den Beschlüssen vom 20.08.2002 (Nr. 474/02) und 29.10.2002 (Nr. 646/02) hat der Berliner Senat die Ziele der E-Government - Entwicklung auf der Grundlage des Masterplans festgelegt und die Verwaltung beauftragt, auf der Grundlage des "Masterplans E-Government" folgende Handlungsfelder (8-Punkte-Programm) zu bearbeiten:

1. Entwicklung von E-Government - Anwendungen für Bürgerinnen und Bürger sowie Wirtschaft
2. Ausbau von zielgruppenorientierten Portalen, Vertriebs- und Zugangswegen
3. Weiterentwicklung der informationstechnischen Infrastruktur für das E-Government
4. Personalentwicklung und personalwirtschaftliche Auswirkungen
5. Gestaltung der rechtlichen und organisatorischen Rahmenbedingungen
6. Finanzierung / Finanzierungsmodelle
7. Intensivierung regionaler und überregionaler Kooperation

8. Planung, Organisation und Steuerung der Entwicklung des E-Government insgesamt

In der Berliner Verwaltung finden sich derzeit folgende (ausgewählte) E-Government-Projekte für die Wirtschaft und die Bürgerinnen und Bürger:

- Ausbau des Berlin-Telefons zur Servicenummer 115 im Rahmen des Aktionsplanes Deutschland-Online. (SenInnSport)
- Umsetzung der EU-Dienstleistungsrichtlinie vom 12. Dezember 2006. Einheitlicher qualifizierter Ansprechpartner, vollständige elektronische Verfahrensabwicklung, Anpassung des dienstleistungsbezogenen Fachrechts und der Verwaltungsverfahren. (SenWTF)
- Einführung der Europäischen Meldeauskunft "RISER" (Registry Information Service on European Residents). (SenInnSport)
- Bereitstellung von Online-Dienstleistungen der Bürgerämter durch das Projekt Virtuelle Bürgerdienste (Online-Bürgeramt). (SenInnSport, Bezirke)
- Elektronische Baugenehmigung: elektronische Unterstützung aller Geschäftsprozesse der Berliner Bauaufsicht von der Beantragung durch den Bauherren über die Beteiligung aller Behörden und die Bescheiderteilung bis zur Archivierung. (SenStadt)
- Fortführung und Abschluss der "Berliner Justizreform" (effektive, schnell arbeitende und bürgernahe Justiz), Verkürzung der Dauer von Gerichtsverfahren. (SenJust)
- Erarbeitung und Veröffentlichung verbindlicher Qualitätsstandards für häufig nachgefragte Verwaltungsleistungen (z.B. für die Zeiträume von der Beantragung bis zur abschließenden Bearbeitung). (alle Verwaltungen)
- Eröffnung weiterer Verfahren für Online-Dienste einschließlich Formularservice. Online-Kfz-Zulassungsservice. (SenInnSport)
- Ausgabe aller Urkunden der Standesämter direkt über Berlin.de. (Bezirk Neukölln)
- Verbesserung der Information über Rechtsvorschriften zur Sozialhilfe durch Veröffentlichung im Internet. (SenIAS)
- Online-Verfahren Schwerbehindertenantrag (SenIAS)
- Unterstützung der Schulen in erweiterter Verantwortung durch verstärkten Einsatz von Informationstechnik im Projekt eAdministration@School Berlin. (SenBWF)
- E-Government-Lösung im IT-Verfahren Gewerbedatenbank. (SenWTF)
- E-Government-Lösung Starter-Center bei IHK und HWK. (SenWTF)
- Aufbau einer Redaktion "Wirtschaftsportal". (SenWTF)
- Schaffen wirtschaftsfreundlicher Bedingungen durch Vereinheitlichung und Verzahnung der Strukturen der Wirtschaftsförderung. Stärkere Verzahnung von Berlin Partner mit der zentralen Anlauf- und Koordinierungsstelle (ZAK) und den bezirklichen Anlauf- und Koordinierungsstellen. Abbau von Bürokratie, Entscheidungswege verkürzen. (SenWTF)

- Entlastung von Unternehmen von überflüssigen, durch Bürokratie verursachten Kosten durch Bürokratiemessung. (SenWTF)

Informationen zu diesen und anderen Projekten sind auf der Internetseite der Stadt Berlin (www.berlin.de) zum Stichwort „E-Government“ zu finden.

10.1.1. Beziehungen

	Bürger	**Verwaltung**	**Wirtschaft**
Bürger	Consumer to Consumer C2C	Consumer to Government C2G	Consumer to Business C2B
Verwaltung	Government to Consumer G2C	Government to Government G2G	Government to Business G2B
Wirtschaft	Business to Consumer B2C	Business to Government B2G	Business to Business B2B
	E-Commerce	**E-Government**	**E-Business**

10.1.2. Verfahrenssicherheit

Bei behördlichen Angelegenheiten stellen sich immer wieder die gleichen grundlegenden Fragen:

- Wie erkenne ich, mit wem ich kommuniziere?
- Sind die Daten unverfälscht eingegangen?
- Können die Daten von Dritten beim Transport mitgelesen werden?
- Wie kann digital die Schriftform gewahrt werden?

Beispiel: Ein Bürger sendet eine E-Mail an das zuständige Bürgeramt.

Schon alleine bei diesem simplen Vorgang müssen folgende Fragen geklärt werden:

- Wer hat die E-Mail gesendet?
- Ist der angegebene Absender tatsächlich die Person, für die sie sich ausgibt?
- Wurde die E-Mail beim Transport mitgelesen und/oder sogar verändert?
- Hat der Empfänger die E-Mail tatsächlich erhalten?

Einen wertvollen Beitrag leistet der seit dem 01. November 2010 erhältliche elektronische Personalausweis in Verbindung mit einem entsprechenden Lesegerät.

Mit dem neuen Personalausweis wird ein Standard-Identitätsausweis für die digitale Welt geschaffen, mit dem Sie sich online schnell, einfach und sicher ausweisen können. Das liegt an dem integrierten "Radio Frequency"-Chip (Funkchip oder auch RF-Chip). Auf diesem werden neben den persönlichen Daten, die auf dem Ausweis aufgedruckt sind, unter anderem auch das Foto sowie eine PIN digital gespeichert. Außerdem besteht für Sie die Möglichkeit – wenn gewünscht – auf dem Chip Fingerabdrücke abspeichern zu lassen.

Zusätzlich kann man sich mit ihm digitale Dokumente rechtsverbindlich unterschreiben. Somit können Behördengänge und meist damit verbundene lange Wartezeiten vermieden werden.

Auch die seit Mitte 2010 erhältliche De-Mail-Adresse, bei der man sich einem sehr aufwendigen, mehrstufigen Autorisierungsverfahren im Anmeldeverfahren unterziehen muss, ist ein elementarer Baustein. Sinn und Zweck von De-Mail ist es, grundlegende Sicherheitsfunktionen für den sicheren Austausch elektronischer Nachrichten einfacher anwendbar zu machen und damit deren rasche Verbreitung zu fördern.

Für ein noch höheres Sicherheitsniveau können zusätzliche Sicherheitstechnologien eingesetzt werden. Selbstverständlich können auch im Rahmen von De-Mail elektronische Signaturen zum Einsatz kommen.

Problematisch ist aus der Sicht der Betreiber von E-Government-Plattformen, dass die bislang in sich geschlossenen Verwaltungsnetze nach außen geöffnet werden müssen, wodurch diese leichter angreifbar sind.

Es müssen künftig noch mehr (personenbezogene) Daten, aber auch Verbindungsdaten elektronisch gespeichert werden.

10.2. E-Commerce

Elektronischer Handel (auch Internetverkauf, Elektronischer Marktplatz, Virtueller Marktplatz) ist der virtuelle Einkaufsvorgang via Datenfernübertragung innerhalb der Distributionspolitik des Marketings. Hierbei wird über das Internet eine unmittelbare Handels- oder Dienstleistungsbeziehung zwischen Anbieter (Verwaltung) und Abnehmer (Bürger) abgewickelt.

Die Besonderheiten beim Elektronischen Handel der Distribution im Marketing-Mix gegenüber den traditionellen Vertriebskanälen sind die enorme Flexibilität auf der Angebotsseite, sowie eine erhebliche Reduzierung der Transaktionskosten mit Geschäftspartnern. Es werden beispielsweise auch Reise- oder Telefonkosten in der Kundenakquisition und Leistungspräsentation gesenkt. Die räumlichen Distanzen sind bei physischen Leistungen dennoch zu überwinden und erfordern entsprechende Logistikkapazitäten.

Heute versteht man unter Elektronischem Handel in der Regel alle Methoden der Abwicklung von Geschäften und administrativen Vorgängen über elektronische Kanäle, wobei das Internet oder zumindest die im Internet verwendeten Techniken und Protokolle eine wesentliche Rolle spielen und die Informationstechnologie gemeinhin als Voraussetzung angesehen wird.

Der Begriff des Onlineshop ist hierbei die eingedeutschte englische Bezeichnung für den Warenvertrieb durch die Internetpräsenz eines Händlers. Weitere Bezeichnungen für die organisatorische Umsetzung sind Webshop und E-Shop (für Elektronik-Shop) bzw. selten verdeutscht E-Laden.
Dem einfachen Verkaufsabschluss wird aus individualpsychologischer Sicht beim Internetverkauf eine besonders hohe Bedeutung beigemessen, weil der Kunde seinen Warenkorb ohne Angst vor Datenverlust und Spionage seiner Zahlungsdaten begleichen können soll.

Die klassischen Zahlungsarten Vorkasse, Rechnung, Nachnahme und Kreditkarte machen in Deutschland weiterhin einen Großteil der Zahlungen aus. Häufig findet auch das bekannte Bankeinzugsverfahren Anwendung, da die Hemmschwelle zur Übermittlung der Kontoverbindung oft geringer ist, als die zur Anwahl einer Mehrwertnummer oder die Angabe der Kreditkartendaten.

Micropaymentsysteme[15] haben es dagegen schwer, sich zu etablieren. Ein anonymes Bezahlverfahren z. B. ist giropay. Der Zahlungspflichtige wird vom Online-Shop auf die Seite seines Kreditinstituts geleitet und tauscht die persönlichen Daten ausschließlich mit seiner Bank aus.

Den höchsten Bekanntheitsgrad bei speziell für das Internet entwickelten Zahlungssystemen hat Paypal erreicht, ein Tochterunternehmen des Auktionshauses Ebay. Auch das HBCI[16]-Banking ist verbreitet und wird bislang als „sicher“ eingestuft.

Der Kunde wird in vielen Fällen in den Verkaufsprozess mit einbezogen. Beispielsweise kann das Briefporto online erworden werden, die bildhafte Darstellung von Briefmarken wird mehr und mehr durch maschienenlesbare „Briefmarken“ ersetzt.

[15] bezeichnet ein Zahlungsverfahren geringer Summen.
[16] Homebanking Computer Interface (**HBCI**) ist ein offener Standard für den Bereich Electronic Banking und Kundenselbstbedienung

Die Fahrscheine der Deutschen Bahn können am heimischen PC ausgedruckt werden und die enthaltenen Daten in Form eines „Strichcode“ dargestellt. Lesegeräte prüfen die Echtheit des „Fahrscheins“.

Im Einzelhandel werden die Produkte mit RFID17-Chips versehen, sodass perspektivisch keine Verkäuferin die Produkte mit Hilfe eines Scanners einlesen muss, sondern der vollgepackte Einkaufswagen lediglich durch ein „Tor“ geschoben werden muss. Die RFID-Chips an den Produkten funken ihre Information an eine Kasse – der Kunde muss nur noch bezahlen. Das Ein- und Auspacken des Einkaufswagens an der Kasse gehört der Vergangenheit an.

10.3. E-Learning

Unter E-Learning (auch eLearning, englisch electronic learning – elektronisch unterstütztes Lernen), auch E-Lernen genannt, werden – nach einer Definition von Michael Kerres – alle Formen von Lernen verstanden, bei denen digitale Medien für die Präsentation und Zusammenstellung von Lernmaterialien und/oder zur Unterstützung zwischenmenschlicher Kommunikation zum Einsatz kommen.

Für E-Learning finden sich als Synonyme auch Begriffe wie Online-Lernen, Telelernen, Computer Based Training, multimediales Lernen, Open and Distance Learning, computergestütztes Lernen u.a.

10.3.1. Blended Learning

Der Begriff „integriertes Lernen“ oder englisch „Blended Learning“ bezeichnet einen Ansatz der Lernorganisation, bei dem die Vorteile von Präsenzveranstaltungen und E-Learning kombiniert werden.

Direkt übersetzt heißt Blended Learning "vermischtes Lernen". Bei dieser Form werden verschiedene Lernmethoden, Medien sowie lerntheoretische Ausrichtungen miteinander kombiniert.

Blended Learning bezeichnet also eine Lernorganisation, bei der die Vorteile durch die Kombination verschiedener Medien und Methoden verstärkt und die Nachteile minimiert werden können.

Das auch „Hybride Lernarrangements“ genannte Konzept verbindet die Effektivität und Flexibilität von elektronischen Lernformen mit den sozialen Aspekten der Face-to-Face-Kommunikation.

Es bezeichnet damit eine Lernform, die eine didaktisch sinnvolle Verknüpfung von „traditionellem Klassenzimmerlernen“ und modernen Formen von E-Learning anstrebt. Besonders wichtig ist, dass das eine ohne dass andere nicht funktioniert - die Präsenzphasen und Online-Phasen müssen also optimal aufeinander abgestimmt sein!

10.3.2. Web Based Training

Web Based Training (WBT) ist ein Oberbegriff, unter dem sich auf Internet-Technologie basierte Lernprogamme einordnen lassen.

Das WBT ist eine Weiterentwicklung des Computer Based Training (CBT). Es werden Lerneinheiten nicht auf einem Datenträger verbreitet, sondern von einem Webserver online mittels Internet oder Intranet abgerufen.

Die Einbettung ins Netz bietet vielfältige weiterführende Möglichkeiten der Kommunikation und Interaktion des Lernenden mit den Mitlernern. Wenn das WBT von einem Dozenten/Tutor moderiert wird, liegt moderiertes WBT (mWBT) vor. Im mWBT werden E-Mail, News, Chats, Materialarchive und Diskussionsforen vom Dozenten mit dem WBT verknüpft und Lernende werden durch den Dozenten zur Nutzung angeleitet und motiviert.

Zusätzlich können datenintensive Audio- und Videosignale live gestreamt über synchrone Konferenzplattformen verbreitet werden.

In der betrieblichen Weiterbildung großer Firmen spielen WBTs heute von allen E-Learning Technologien die größte Rolle. Für mittlere und erst recht kleine Firmen ist der finanzielle Aufwand hingegen zu groß. Die Voraussetzung für Web Based Training ist ein leistungsfähiges Intranet. Da WBTs relativ wartungsfreundlich sind, sind sie insbesondere für Inhalte, die sich schnell ändern können, das bevorzugte Medium (z. B. Versicherungsbranche).

Oftmals wird eine inhaltliche Verzahnung mit Präsenzseminaren angestrebt (vgl. Blended Learning).

10.4. Elektronische Signatur

Ein erster Weg hier eine für beide Seiten sichere Lösung zu finden, ist die qualifizierte elektronische Signatur.

Unter einer elektronischen Signatur versteht man Daten, mit denen man den Unterzeichner bzw. Signaturersteller identifizieren kann und sich die Integrität der signierten, elektronischen Daten prüfen lässt. Die elektronische Signatur erfüllt somit technisch gesehen den gleichen Zweck wie eine eigenhändige Unterschrift auf Papierdokumenten.

10.4.1. Formen der elektronischen Signatur

Das Signaturgesetz (SigG) übernimmt im Wesentlichen die Definitionen der europäischen Richtlinie[17] und unterscheidet ebenso wie diese zwischen den folgenden Formen von elektronischen Signaturen:

3. einfache (allgemeine) elektronische Signatur
4. fortgeschrittene elektronische Signatur
5. qualifizierte elektronische Signatur.

Jede Signatur steht für eine bestimmte Qualitätsstufe. Je höherwertiger die Signatur, desto mehr Bedeutung hat sie für den Rechtsverkehr und desto größer ist ihre Funktionalität.

An eine einfache (d.h. nicht fortgeschrittene) elektronische Signatur werden keine besonderen Anforderungen gestellt. So gelten z. B. die Angaben des Urhebers oder Absenders ohne digitale Signatur als „einfache" Signatur. Einfache elektronische Signaturen können gemäß § 127 BGB für formfreie Vereinbarungen eingesetzt werden.

Für eine fortgeschrittene elektronische Signatur übernimmt § 2 Nr. 2 SigG im Wesentlichen die Definition der Richtlinie:

> Eine fortgeschrittene Signatur muss mit dem Signaturschlüssel des Signaturerstellers und mit Mitteln, die unter seiner alleinigen Kontrolle stehen, erstellt worden sein, und seine Identifizierung ermöglichen.

Der Begriff „Signaturschlüssel" bezieht sich hierbei nicht notwendigerweise auf kryptographische Schlüssel. Für die Identifizierbarkeit des Signaturerstellers ist nicht zwingend ein Zertifikat erforderlich, so dass z. B. auch mit PGP[18] fortgeschrittene elektronische Signaturen erstellt werden können. Fortgeschrittene elektronische Signaturen können gemäß § 127 BGB für formfreie Vereinbarungen eingesetzt werden.

Nur Dokumente mit einer qualifizierten elektronischen Signatur gemäß § 2 Nr. 3 SigG können als elektronische Form eine per Gesetz geforderte Schriftform auf Papier ersetzen, vgl. § 126 a BGB. In Übereinstimmung mit der europäischen Richtlinie ist eine qualifizierte elektronische Signatur eine fortgeschrittene elektronische Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruht und mit einer sicheren Signaturerstellungseinheit (SSEE) erstellt wurde.

Der Signaturschlüssel darf dabei ausschließlich in der SSEE gespeichert und angewendet werden. Die Übereinstimmung der SSEE mit den Vorgaben des Signaturgesetzes muss durch eine anerkannte Stelle geprüft und bestätigt werden. Dagegen ist auch für qualifizierte elektronische Signaturen eine Prüfung und Bestätigung

[17] Richtline 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

[18] Pretty Good Privacy, auf deutsch etwa „Ziemlich Gute Privatsphäre" ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung.

der Signaturanwendungskomponente, welche Signatursoftware, Treiber und Chipkarten-Leser umfasst, nicht zwingend vorgeschrieben.

10.5. Voice over IP

Unter „Voice over IP“ (kurz VoIP) oder auch der „IP-Telefonie“, eine Kurzform für die Internet-Protokoll-Telefonie, auch Internet-Telefonie, versteht man das Telefonieren über Computernetzwerke, welche nach Internet-Standards aufgebaut sind.

Dabei werden für Telefonie typische Informationen, d. h. Sprache und Steuerinformationen beispielsweise für den Verbindungsaufbau über ein auch für Datenübertragung nutzbares Netz übertragen.

Bei den Gesprächsteilnehmern können sowohl Computer, auf IP-Telefonie spezialisierte Telefonendgeräte, als auch über spezielle Adapter angeschlossene klassische Telefone die Verbindung ins Telefonnetz herstellen.

IP-Telefonie ist eine Technologie die es ermöglicht, den Telefondienst auf dieser IP-Infrastruktur zu realisieren, so dass diese die herkömmliche Telefontechnologie samt ISDN, Netz und allen Komponenten ersetzen kann.

Zielsetzung dabei ist eine Reduzierung der Kosten durch ein einheitlich aufgebautes und zu betreibendes Netz, wodurch sich für die Betreiber Kostenvorteile ergeben, die an den Endverbraucher weitergegeben werden können. Aufgrund der hohen Einsatzdauer klassischer Telefoniesysteme und der notwendigen Neuinvestitionen für IP-Telefonie wird der Wechsel bei bestehenden Anbietern oft als lang andauernder, gleitender Übergang realisiert. Währenddessen existieren beide Technologien parallel (sanfte Migration).

Daraus ergibt sich ein deutlicher Bedarf an Lösungen zur Verbindung beider Telefoniesysteme (z. B. über VoIP-Gateways) und die Notwendigkeit zur gezielten Planung des Systemwechsels unter Berücksichtigung der jeweiligen Möglichkeiten für Kosten- und Leistungsoptimierung.

Auch in der Berliner Landesverwaltung wird das interne Telefonnetz nach und nach auf diese Technik umgestellt. Das neue Berliner Landesnetz Next Generation (BeLa-NG) beseitigt damit die letzten Engpässe und ermöglicht eine sichere Kommunikation für mehr als 50.000 Anwender.

Das „Berlin Telefon 115“ nutzt bereits diese Technik: Nimmt die Telefonzentrale den Anruf über VoIP entgegen, öffnet sich eine elektronische Notiz (Ticket), in die alle Informationen des Anrufers eingetragen werden. Muss das Anliegen an eine andere Stelle übergeben werden, haben auch dort die Mitarbeiter mit der Übernahme des Anrufs sofort Zugriff auf die eingegebenen Informationen.

Der Bürger braucht somit sein Anliegen nicht ein zweites Mal vorzutragen und die Verwaltungsmitarbeiter erhalten auf einen Blick alle Informationen, die für die Bearbeitung erforderlich sind.

Natürlich gibt es bei dieser Technik auch Risiken: Zum Beispiel Spam über Internet-Telefon (SPIT). Die aus der täglichen E-Mail-Praxis bekannte Spamflut droht auch auf die VoIP-Telefondienste im Internet „herüberzuschwappen".

Das BeLa-NG übermittelt und empfängt Anrufe, die nicht von Teilnehmern aus dem eigenen Netz kommen, nur über herkömmliche Telefonleitungen und ist daher vor der Spamflut geschützt. Diese „externen" Teilnehmer werden über ein zentrales Gateway in das Datennetz übertragen.

VoIP ist nicht nur eine Alternative zur bisherigen Telefonie, sondern kann diese in der Zukunft vollständig ablösen. „Voipen" ist seit der 24. Auflage ein offizielles Verb im Duden.

Die großen Telefonkonzerne haben bereits angekündigt, zukünftig auf VoIP umzusteigen; die Deutsche Telekom hat hierfür das Jahr 2012 als Zieltermin für eine Ablösung des bisherigen Telefonnetzes genannt.

10.6. Telearbeit

Unter dem Begriff Telearbeit werden verschiedene Arbeitsformen zusammengefasst, bei denen Mitarbeiter zumindest einen Teil der Arbeit außerhalb der Gebäude des Arbeitgebers verrichten (es muss kein Angestelltenverhältnis bestehen).

Oftmals werden die Arbeitsergebnisse dabei dem Arbeitgeber über digitale Kanäle übermittelt. Dazu werden häufig Kommunikationsgeräte wie Computer, Fax und Telefon genutzt. Vereinbarungen über Arbeitsziele, Termine usw. werden mit dem Arbeitgeber, dem Arbeitsteam oder beiden getroffen.

Das Unternehmen hat bei Telearbeit unter anderem den Vorteil, dass es weniger Büroflächen zur Verfügung stellen muss. Außerdem können die Kompetenzen von Mitarbeitern weiter genutzt werden, die nicht regelmäßig im Büro erscheinen können, zum Beispiel wegen der Kinderbetreuung.

Es werden üblicherweise verschiedene Formen der Telearbeit unterschieden:

- Bei der *Teleheimarbeit* (häufig auch als Home Office genannt, im englischen jedoch als working at home bezeichnet) verrichtet der Arbeitnehmer die gesamte Arbeit als Heimarbeit in seiner eigenen Wohnung.

Ein Arbeitsplatz in den Räumlichkeiten des Unternehmens existiert nicht. Beliebt ist dieses Arbeitsmodell bei jungen Müttern, denen so der Wiedereinstieg in das Berufsleben erleichtert wird, aber auch bei jungen Vätern.

Die Arbeitsleistung kann verteilt erbracht und die Kinder trotzdem versorgt werden. Für den Arbeitgeber ergibt sich der Vorteil, dass Fach- und Firmenwissen sowie eine geschätzte Arbeitskraft erhalten bleiben.

- *Alternierende Telearbeit* ist die vorherrschende Variante der Telearbeit. Hierbei wird abwechselnd zu Hause und im Unternehmen gearbeitet.

  Das Unternehmen stellt für die Arbeit mehreren Personen einen Arbeitsplatz zur Verfügung, der dann von ihnen zu unterschiedlichen und miteinander abgesprochenen Zeiten genutzt wird. Auch dieses Arbeitsmodell ist besonders bei jungen Eltern beliebt (s. o.).

- Die *Mobile Telearbeit* wird hauptsächlich von Vertretern, Kundenbetreuern und ähnlichen Berufsgruppen praktiziert. Hierbei steht die Tätigkeit an wechselnden Arbeitsorten (z. B. in der Kundenwohnung) sowie u. U. der Fernzugriff auf die unternehmensinterne IT-Infrastruktur im Mittelpunkt.

Telearbeit stellt verschiedene Anforderungen an alle Beteiligten. So muss ein geeigneter Arbeitsplatz zu Hause mit privaten Mitteln oder vom Arbeitgeber eingerichtet werden.

Dabei müssen auch die Aspekte des Arbeitsschutzes und der Arbeitssicherheit sowie versicherungstechnische Probleme, die sich aus den verschiedenen rechtlichen Bestimmungen ergeben, Berücksichtigung finden.

Neben den bekannten Vorteilen (z. B. weniger Zeitverlust durch Arbeitswege, bessere Vereinbarkeit von Familie und Beruf) bringt Telearbeit auch unterschiedliche Gefahren mit sich.

So müssen Telearbeiter bereit sein, stärker mit den übrigen Beteiligten zu kommunizieren und die erforderliche Selbstdisziplin aufbringen, anfallende Arbeiten termingerecht zu erledigen.

Selbstausbeutung und Vereinsamung

Oftmals werden auch eine drohende Selbstausbeutung und Vereinsamung von Telearbeitern genannt, der durch geeignete Maßnahmen Rechnung getragen werden muss. Der Arbeitgeber hingegen muss einer ergebnisorientierten Arbeit positiv gegenüberstehen und auf die tradierten Kontrollfunktionen zu Gunsten eines stärkeren Vertrauens zu seinen Dienstkräften verzichten können.

Als einzig tragfähiges Managementkonzept bei der Telearbeit gilt das Management by Objectives. Dabei kommt dem Prinzip der Zielverein-

barung die größte Bedeutung zu. Vor- und Nachteile dieses Arbeitszeitmodells sind in weiten Bereichen des Arbeitslebens immer noch umstritten.

Bestehende politische Zielvorgaben sowie raumstrukturelle, kulturelle und rechtliche Randbedingungen haben einen großen Einfluss auf die Verbreitung und die Auswirkungen von Telearbeit.

So führen in den am dichtesten besiedelten Gebieten in den Niederlanden beispielsweise viele Firmen Telearbeit und flexible Arbeitszeitmodelle ein, um den Mitarbeitern lange Anfahrtszeiten und Zeitverlust durch Verkehrsstaus in den Spitzenzeiten zu ersparen.

In der Berliner Landesverwaltung haben bisher nur wenige Verwaltungen Möglichkeiten zur Telearbeit geschaffen. Politisch wird Telearbeit zwar gefördert, bisher jedoch nicht gezielt als politische Maßnahme zur Senkung der Verkehrsnachfrage eingesetzt.

Fragen zur Selbstkontrolle:

46. Welchen Sinn soll E-Government erfüllen?
47. Definieren Sie „E-Government“.
48. Nennen Sie E-Government-Projekte in der Berliner Verwaltung.
49. Welche Probleme gibt es bei der Einführung von E-Government?
50. Nennen Sie die Formen einer elektronischen Signatur?
51. Erläutern Sie die Elemente des NSM.
52. Nennen Sie die Kernelemente des NPM

11. Auswirkungen der Informationstechnik

Die Informationsgesellschaft

In früheren Zeiten trafen die Informationen in einer angemessenen Geschwindigkeit auf den Einzelnen, manchmal kamen sie sogar zu langsam, es herrschte also ein Informationsdefizit - wer erinnert sich nicht an die Frage „Was gibt es Neues?“. Heute dagegen treffen immer mehr Informationen in immer kürzerer Zeit auf den Einzelnen.

Diese Informationen wollen erfasst, ausgewertet und wenn nötig zur späteren Verfügbarkeit vorgehalten werden. Besonders beruflich ist es notwendig, möglichst viele Informationen sofort präsent zu haben. „Was, das wissen Sie noch nicht?“ ist heute quasi schon eine Abmahnung für alle, die nicht den aktuellen Informationsstand haben. Eine Situation, die man sich besonders im Berufsleben nicht häufig erlauben kann. Berufliches Fortkommen setzt das Wissen über Art, Umfang und Nutzungsmöglichkeit des aktuellen Informationspools voraus.

Aber sind diese Anforderungen überhaupt erfüllbar?

Bei der Beantwortung dieser Frage sollte man folgende Punkte berücksichtigen:

- Das Weltwissen verdoppelt sich alle fünf Jahre.
- Das Wissen eines Spezialisten ist nach zwei Jahren ohne Fortbildung nicht mehr aktuell.
- Die Bedienungsanleitung eines Atom-U-Bootes wiegt ca. 18.000 kg, passt aber auf eine CD.
- Auf den Bürger einer durchschnittlich kulturell erschlossenen Nation treffen jährlich (statistisch gesehen) 480.000.000.000.000 Wörter aus den informationsspendenden Medien und Interaktionen (Fernsehen, Radio, Zeitung, Werbung, Unterhaltung etc.).
- Von dem Wahrgenommenen vergisst man 80 Prozent innerhalb von 24 Stunden.
- Es werden Informationen angehäuft, bei denen die Notwendigkeit zu bezweifeln ist: So kommen die zehn Gebote mit 279 Worten und die amerikanische Unabhängigkeitserklärung mit 300 Worten aus; die Vorschrift über die Einfuhr von Karamellbonbons in die EG umfasst 25.911 Worte.
- Technische Hilfsmittel werden immer leistungsfähiger, schneller aber auch komplexer.

Die Folge wird sein:

- Wer sich den Zugang zu den Informationen nicht leisten kann, wird sozial absteigen.
- Wer Informationen hat und/oder kontrolliert, hat Macht.
- Nationale Kulturen verlieren an Bedeutung; so glauben heute 40 % der Kinder in Schweden im Alter zwischen 6 und 10 Jahren,

dass Menschen ausschließlich durch Mord und Totschlag sterben.
- Die aufzunehmenden Informationen werden selektiert, das Spezialistentum nimmt zu.
- Berufsbilder werden sich immer schneller verändern; Computerunterstützung wird in allen Berufen selbstverständlich.
- Wer nicht möglichst schon in der Schule den Umgang mit Geräten der Informationstechnik erlernt, hat später kaum eine Chance diesen Rückstand aufzuholen.

Zur Bewältigung der Informationsflut gibt es in Organisationen verschiedene Strategien:

- Personalvermehrung
- Änderung der Aufbau- und Ablauforganisation
- Informationsreduktion bis hin zur Informationsvermeidung
- Informationsrecycling
- Informationsumleitung
- Informationsnegierung

Meist wird das Anwachsen der zu verarbeitenden Informationsmengen als eine Art Naturgesetz gesehen, alle Kräfte werden zur Bewältigung der anfallenden Informationsmengen eingesetzt, nicht zu deren Verminderung.

Seltener wird die „horizontale und vertikale Integration“ der Büroarbeit versucht. Darunter versteht man eine Verringerung der Anzahl der bei der Verarbeitung von Informationen beteiligten Stellen in den einzelnen Ebenen ebenso, wie auch die vertikale Kompression der Organisations-/Hierarchiestruktur.

Die damit verbundenen Änderungen werden alle Büroberufe betreffen. Der Sachbearbeiter wird Schreibdiensttätigkeiten ebenso übernehmen wie andere Aufgaben, die aus den Arbeitsebenen zwischen Posteingang und -ausgang auf ihn konzentriert werden.

Auf Dauer ist diese Integration aber nur dann als ein geeignetes Mittel zur Informationsbewältigung anzusehen, wenn sie mit einem oder mehreren der oben zusätzlich erwähnten Ansatzpunkte zur Informationsbewältigung kombiniert wird.

11.1. IT-Regelwerk

Ziel des im Rahmen der Umsetzung des Senatsbeschlusses zu den Ergebnissen der Expertenkommission Staatsaufgabenkritik für den Bereich Informationstechnologie vom 30. April 2002 entwickelten IT-Regelwerks ist es, den Einsatz von Informationstechnik so zu steuern, dass Effizienz und Effektivität des Verwaltungshandelns gefördert werden.

Das Regelwerk schafft einheitliche Rahmenbedingungen für Planung, Beschaffung bzw. Entwicklung und Einsatz von IT in der Berliner Verwaltung unter Beachtung dezentraler Verantwortlichkeiten für die Ergebnisse des Verwaltungshandelns.

Bestandteile des IT Regelwerks sind:

- das Gesetz über die Anstalt öffentlichen Rechts IT-Dienstleistungszentrum Berlin (ITDZ), vormals „§-26-LHO-Betrieb“ - Landesbetrieb für Informationstechnik (LIT)
- darin: Eine Anpassung des Zuständigkeitskatalogs des Allgemeinen Zuständigkeitsgesetzes durch die die bisher bestehende Regelungskompetenz des Senats auf dem Gebiet der IT in der Verwaltung auf die Festlegung zwingend notwendiger Vorgaben für den IT-Einsatz erweitert wird
- die Verwaltungsvorschriften für die Steuerung des IT-Einsatzes in der Berliner Verwaltung

Das Abgeordnetenhaus hat das Gesetz über die Anstalt öffentlichen Rechts IT-Dienstleistungszentrum Berlin (ITDZ) am 19. November 2004 beschlossen. Es wurde am 30. November 2004 im GVBl. Veröffentlicht.

Mit dem genannten Gesetz ist der zentrale Baustein für ein modernes und zukunftsorientiertes Regelwerk zum Einsatz von Informationstechnik in der Berliner Verwaltung geschaffen worden.

Die Verwaltungsvorschriften für die Steuerung des IT-Einsatzes in der Berliner Verwaltung gelten seit 1. Oktober 2004. Sie geben Auskunft über die Steuerungsinstrumente für den IT-Einsatz in der Berliner Verwaltung und deren Zusammenwirken. Die Verwaltungsvorschriften konkretisieren insbesondere die erwähnte Änderung des AZG. Mit Inkrafttreten der IT-Organisationsgrundsätze wurden die Organisationsstrukturen in Hauptverwaltung und Bezirken entsprechend angepasst.

11.2. IT-Organisationsgrundsätze

Der Senat hat in seiner Sitzung am 27.06.2006 – nach Zustimmung durch den Rat der Bürgermeister – die IT-Organisationsgrundsätze auf Basis der VV IT-Steuerung beschlossen. Sie ersetzen die am 19.12.2005 ausgelaufene IT-Organisationsrichtlinie und sind ab sofort einheitlich anzuwenden.

Die IT-Organisationsgrundsätze legen aufbauorganisatorische Grundstrukturen und Rollen für den Bereich des IT-Einsatzes fest und konkretisieren die entsprechenden Vorgaben aus der VV IT-Steuerung. Dabei wird den sich stetig verändernden technischen und organisatorischen Rahmenbedingungen soweit möglich Rechnung getragen. Auf dieser Grundlage könne effiziente, flexible und adäquate Organisationsstrukturen für die Planung und den Einsatz von Informa-

tionstechnik in der Berliner Verwaltung aufgebaut und arbeitsfähig gemacht werden.

Die IT-Organisationsgrundsätze tragen wesentlich zur Vereinheitlichung der dezentralen Aufgabenwahrnehmung und Arbeitsweisen bei.

11.3. Cloud Computing

Mit Cloud Computing wird der Ansatz verfolgt die Rechenkapazität, den Datenspeicher, fertige Software dynamisch an den Bedarf des Nutzers angepasst über ein Netzwerk zur Verfügung zu stellen. Als Service wird eine Programmierumgebung zur Verfügung gestellt. Die Verarbeitung der Daten erfolgt somit nicht mehr auf dem heimischen Computer sondern auf einem entfernten Server des Cloudanbieters. Dadurch wird die Anwendungen für den Nutzer transparent und verblasst somit gewissermaßen in einer „Wolke“.

Die Abrechnung erfolgt nutzungsabhängig, da nur tatsächlich genutzte Dienste bezahlt werden müssen. Ein weiterer Punkt des Konzeptes ist, dass die Bereitstellung basierend auf der Kombination aus virtualisierten Rechenzentren und modernen Webtechnologien wie Webservices vollautomatisch erfolgen kann und somit keinerlei Mensch-Maschine-Interaktion mehr erfordert.

Bei „Cloud Computing“ geht es aber auch darum, alles als dynamisch nutzbaren Dienst zur Verfügung zu stellen, sei es nun Buchhaltung, einfachste von Menschen verrichtete Arbeit, eine fertige Softwarelösung oder beliebige andere Lösung.

Im Zentrum steht dabei die Illusion der unendlichen Ressourcen, die völlig frei ohne jegliche Verzögerung an den tatsächlichen Bedarf angepasst werden können.

Vereinfacht kann das Konzept wie folgt beschrieben werden: Ein Teil der IT-Landschaft wird durch den Anwender nicht mehr selbst betrieben oder bereitgestellt, sondern von einem oder mehreren Anbietern als Dienst gemietet.

Die Anwendungen und Daten befinden sich dann nicht mehr auf dem lokalen Rechner oder im Firmenrechenzentrum, sondern in der Wolke (engl. „cloud“). Das Bild der Wolke wird in Netzwerkdiagrammen häufig zur Darstellung eines nicht näher spezifizierten Teils des Internets verwendet.

Der Zugriff auf die entfernten Systeme erfolgt über ein Netzwerk, beispielsweise das des Internets. Es gibt aber im Kontext von Firmen

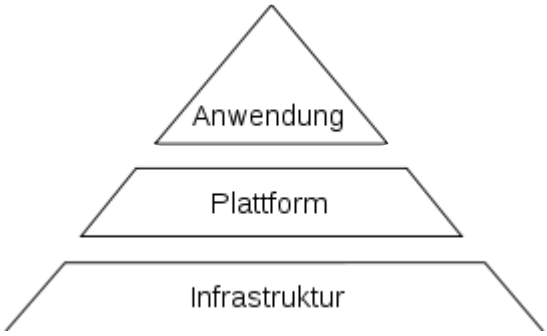
auch sogenannte „Private Clouds“, bei denen die Bereitstellung über ein firmeninternes Intranet erfolgt.

11.3.1. Architektur

Die Geschichte von „Cloud Computing“ gibt es erst seit kurzer Zeit, sodass es noch keine eindeutige Definition des Begriffes gibt. Am besten lässt sich die Architektur in der Form einer Pyramide darstellen:

Infrastruktur

Die Infrastruktur oder „Cloud Foundation“ stellt die unterste Schicht dar. Hier werden beispielsweise die virtuellen Server zur Verfügung gestellt. Dadurch erhält man den Vorteil, dass die Hardware je nach Anforderungen beliebig um weitere Instanzen erweitert oder verkleinert werden kann, was in herkömmlichen Datacentern nicht so einfach möglich ist.



Plattform

Hier steht die Anwendung im Vordergrund. Der Entwickler erstellt die Anwendung und lädt diese auf den Server. Dieser kümmert sich dann selbst um die Aufteilung auf die physischen Server.

Auf der anderen Seite hat der Benutzer kaum oder keine Möglichkeit, den Server selbst zu konfigurieren, da er keinen direkten Zugriff darauf hat. Er muss also die Server nicht administrieren, sondern die Administration wird hier komplett vom Anbieter übernommen, wodurch bei den nutzenden Firmen Kosten der Administration eingespart werden können.

Für den Privatbereich hat der Nutzer den Vorteil, dass auch weniger versierte Anwender problemlos die Computertechnik nutzen können, da sie sich nicht mit Installationsprozessen beschäftigen müssen. Auch das Einspielen regelmäßiger Updates wird durch den Anbieter der Plattform vorgenommen.

Anwendung

Bei der Erstellung von Anwendungen in der „Cloud“ muss auf folgende Probleme geachtet werden:

- Das Design soll modular und serviceorientiert sein.
- Die Last ist unberechenbar, denn über den Erfolg einer Anwendung kann selten eine zuverlässige Aussage gemacht werden.

- Die Anwendung soll dynamisch, verteilt und mandantenfähig sein.

Das anwendungsbasierte Cloud-Konzept wird auch Software-as-a-Service (SaaS) genannt.

Bekannte Beispiele für eine Cloud-Anwendung sind Google Docs, Microsoft Skydrive Office Web Apps und Exchange Online, Sharepoint Online, Livemeeting, Office Communications Online.

11.3.2. Arten von Clouds

Man kann zwischen verschiedenen Arten von „Clouds“ unterscheiden, die je nach Anwendungsfall ihre Berechtigung haben:

Private Cloud

Bei „Private Clouds“ steht im Vordergrund, dass sich sowohl Anbieter als auch Nutzer im selben Unternehmen befinden, wodurch beispielsweise sämtliche Probleme aus dem Bereich Datensicherheit mehr oder minder hinfällig werden. Man unterscheidet dabei folgende Evolutionsstufen:

Exploratory Cloud
Hier steht das Ausprobieren von Cloudfunktionalität innerhalb eines Unternehmens im Vordergrund. Dabei geht es insbesondere darum, Potential und Nachteile für konkrete Anwendungen herauszufinden.

Departmental Cloud
Hierbei handelt es sich um eine Cloud, die sich innerhalb eines Unternehmens auch lediglich innerhalb einer Abteilung befindet. Das bedeutet insbesondere, dass Anbieter und Nutzer innerhalb der gleichen Abteilung zu finden sind. Diese Cloudart dient nicht mehr nur Testzwecken.

Literatur

Arbeitskreis Schuhmann,G. (2001): AdA- Aufstieg durch Ausbildung – handlungsorientiert, Verlag Europa-Lehrmittel, Haan-Gruiten
Arnold, R. (1995): Betriebliche Weiterbildung. Klinckhard; Bad HeilbrunnEnterprise Cloud
Im Gegensatz zur „Departmental Cloud“ stammen hier Anbieter und Nutzer aus unterschiedlichen Unternehmensabteilungen.

Public Cloud

Eine „Public Cloud“ ist eine „Cloud“, die öffentlich ist, d. h. von beliebigen Personen und Unternehmen genutzt werden kann und nicht mehr auf interne Anwendungen einer einzelnen Institution/eines Unternehmens beschränkt ist. Hierbei greifen dann auch vor allem Probleme, die mit Datensicherheit zu tun haben und jeder Akteur muss sich selbst überlegen, wie viele und welche Daten er außerhalb seiner unmittelbaren Kontrolle halten möchte. Auch hier gibt es Unterformen:

Exclusive Cloud
„Exclusive Clouds“ setzen voraus, dass sich sowohl Anbieter als auch Nutzer kennen. Sie handeln feste Konditionen aus und schließen einen Vertrag darüber ab. Es gibt keine Unbekannten.

Open Cloud
Bei „Open Clouds“ kennen sich Anbieter und Nutzer vorher nicht. Dies hat zur Folge, dass der Anbieter sein Angebot ohne direkten Input vom Kunden entwickeln und in Form von SLAs festschreiben muss. Auf Grund der Vielzahl an potentiellen Nutzern müssen auch der gesamte Geschäftsabschluss sowie die Nutzung von Instanzen anbieterseitig vollautomatisch ablaufen. Als Beispiel hierfür wären die Amazon Web Services zu nennen oder auch das Marktplatzmodell von Zimory.

Hybrid Cloud
Ein Unternehmen betreibt eine eigene „Private Cloud“ und nutzt zusätzlich redundante Einheiten, die aktiviert werden, wenn Komponenten in einem Netz einen Defekt aufweisen (Failoverstrategie) oder für Belastungsspitzen eine „Public Cloud“.

Anhang 1: Bundesdatenschutzgesetz

Ausfertigungsdatum: 20.12.1990

Vollzitat:
"Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist"

Stand: Neugefasst durch Bek. v. 14.1.2003 I 66; Zuletzt geändert durch Art. 1 G v. 14.8.2009 I 2814

Fußnote Textnachweis ab: 1.6.1991

Das Gesetz wurde als Art. 1 des Gesetes v. 20.12.1990 I 2954 vom Bundestag mit Zustimmung des Bundesrates beschlossen; § 10 Abs. 4 Satz 3 und 4 ist am ersten Tage des vierundzwanzigsten auf die Verkündung folgenden Kalendermonats, im übrigen am ersten Tage des sechsten auf die Verkündung folgenden Kalendermonats gem. Art. 6 Abs. 2 Satz 1 u. 2 G v. 20.12.1990 I 2954 in Kraft getreten. Das Gesetz wurde am 29.12.1990 verkündet.

Erster Abschnitt
Allgemeine und gemeinsame Bestimmungen

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie

a) Bundesrecht ausführen oder
b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,

3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwenden sind, gehen sie den Vorschriften dieses Gesetzes vor. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

(4) Die Vorschriften dieses Gesetzes gehen denen des Verwaltungsverfahrensgesetzes vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

(5) Dieses Gesetz findet keine Anwendung, sofern eine in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegene verantwortliche Stelle personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt, es sei denn, dies erfolgt durch eine Niederlassung im Inland. Dieses Gesetz findet Anwendung, sofern eine verantwortliche Stelle, die nicht in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum belegen ist, personenbezogene Daten im Inland erhebt, verarbeitet oder nutzt. Soweit die verantwortliche Stelle nach diesem Gesetz zu nennen ist, sind auch Angaben über im Inland ansässige Vertreter zu machen. Die Sätze 2 und 3 gelten nicht, sofern Datenträger nur zum Zweck des Transits durch das Inland eingesetzt werden. § 38 Abs. 1 Satz 1 bleibt unberührt.

§ 2 Öffentliche und nicht-öffentliche Stellen

(1) Öffentliche Stellen des Bundes sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen des Bundes, der bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform. Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Öffentliche Stellen der Länder sind die Behörden, die Organe der Rechtspflege und andere öffentlich-rechtlich organisierte Einrichtungen eines Landes, einer Gemeinde, eines Gemeindeverbandes und sonstiger der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform.

(3) Vereinigungen des privaten Rechts von öffentlichen Stellen des Bundes und der Länder, die Aufgaben der öffentlichen Verwaltung wahrnehmen, gelten ungeachtet der Beteiligung nicht-öffentlicher Stellen als öffentliche Stellen des Bundes, wenn

1. sie über den Bereich eines Landes hinaus tätig werden oder

2. dem Bund die absolute Mehrheit der Anteile gehört oder die absolute Mehrheit der Stimmen zusteht. Andernfalls gelten sie als öffentliche Stellen der Länder.

(4) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter die Absätze 1 bis 3 fallen. Nimmt eine nicht-öf-

fentliche Stelle hoheitliche Aufgaben der öffentlichen Verwaltung wahr, ist sie insoweit öffentliche Stelle im Sinne dieses Gesetzes.

§ 3 Weitere Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Automatisierte Verarbeitung ist die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen. Eine nicht automatisierte Datei ist jede nicht automatisierte Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen zugänglich ist und ausgewertet werden kann.

(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass

a) die Daten an den Dritten weitergegeben werden oder

b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(6) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(6a) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

(7) Verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

(8) Empfänger ist jede Person oder Stelle, die Daten erhält. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

(9) Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben.

(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,

1. die an den Betroffenen ausgegeben werden,

2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

(11) Beschäftigte sind:

1. Arbeitnehmerinnen und Arbeitnehmer,

2. zu ihrer Berufsbildung Beschäftigte,

3. Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitandinnen und Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. nach dem Jugendfreiwilligendienstegesetz Beschäftigte,

6. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

7. Bewerberinnen und Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist,

8. Beamtinnen, Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende.

§ 3a Datenvermeidung und Datensparsamkeit
Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert.

§ 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.

(2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung
dürfen sie nur erhoben werden, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder

2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder

b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

1. die Identität der verantwortlichen Stelle,

2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

§ 4a Einwilligung

(1) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.

(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.

(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

§ 4b Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen

(1) Für die Übermittlung personenbezogener Daten an Stellen

1. in anderen Mitgliedstaaten der Europäischen Union,

2. in anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum oder

3. der Organe und Einrichtungen der Europäischen Gemeinschaften gelten § 15 Abs. 1, § 16 Abs. 1 und §§ 28 bis 30a nach Maßgabe der für diese Übermittlung geltenden Gesetze und Vereinbarungen, soweit die Übermittlung im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen.

(2) Für die Übermittlung personenbezogener Daten an Stellen nach Absatz 1, die nicht im Rahmen von Tätigkeiten erfolgt, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, sowie an sonstige ausländische oder über- oder zwischenstaatliche Stellen gilt Absatz 1 entsprechend. Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Satz 2 gilt nicht, wenn die Übermittlung zur Erfüllung eigener Aufgaben einer öffentlichen Stelle des Bundes aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

(3) Die Angemessenheit des Schutzniveaus wird unter Berücksichtigung aller Umstände beurteilt, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind; insbesondere können die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden.

(4) In den Fällen des § 16 Abs. 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde.

(5) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(6) Die Stelle, an die die Daten übermittelt werden, ist auf den Zweck hinzuweisen, zu dessen Erfüllung die Daten übermittelt werden.

§ 4c Ausnahmen

(1) Im Rahmen von Tätigkeiten, die ganz oder teilweise in den Anwendungsbereich des Rechts der Europäischen Gemeinschaften fallen, ist eine Übermittlung personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen, auch wenn bei ihnen ein angemessenes Datenschutzniveau nicht gewährleistet ist, zulässig, sofern

1. der Betroffene seine Einwilligung gegeben hat,

2. die Übermittlung für die Erfüllung eines Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist,

3. die Übermittlung zum Abschluss oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse des Betroffenen von der verantwortlichen Stelle mit einem Dritten geschlossen wurde oder geschlossen werden soll,

4. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

5. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist oder

6. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Die Stelle, an die die Daten übermittelt werden, ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dessen Erfüllung sie übermittelt werden.

(2) Unbeschadet des Absatzes 1 Satz 1 kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten an andere als die in § 4b Abs. 1 genannten Stellen genehmigen, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist; die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben. Bei den Post- und Telekommunikationsunternehmen ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zuständig. Sofern die Übermittlung durch öffentliche Stellen erfolgen soll, nehmen diese die Prüfung nach Satz 1 vor.

(3) Die Länder teilen dem Bund die nach Absatz 2 Satz 1 ergangenen Entscheidungen mit.

§ 4d Meldepflicht

(1) Verfahren automatisierter Verarbeitungen sind vor ihrer Inbetriebnahme von nicht-öffentlichen verantwortlichen Stellen der zuständigen Aufsichtsbehörde und von öffentlichen verantwortlichen Stellen des Bundes sowie von den Post- und Telekommunikationsunternehmen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach Maßgabe von § 4e zu melden.

(2) Die Meldepflicht entfällt, wenn die verantwortliche Stelle einen Beauftragten für den Datenschutz bestellt hat.

(3) Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei in der Regel höchstens neun Personen ständig mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigt und entweder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(4) Die Absätze 2 und 3 gelten nicht, wenn es sich um automatisierte Verarbeitungen handelt, in denen geschäftsmäßig personenbezogene Daten von der jeweiligen Stelle

1. zum Zweck der Übermittlung,

2. zum Zweck der anonymisierten Übermittlung oder

3. für Zwecke der Markt- oder Meinungsforschung gespeichert werden.

(5) Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen

aufweisen, unterliegen sie der Prüfung vor Beginn der Verarbeitung (Vorabkontrolle). Eine Vorabkontrolle ist insbesondere durchzuführen, wenn

1. besondere Arten personenbezogener Daten (§ 3 Abs. 9) verarbeitet werden oder

2. die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens, es sei denn, dass eine gesetzliche Verpflichtung oder eine Einwilligung des Betroffenen vorliegt oder die Erhebung, Verarbeitung oder Nutzung für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

(6) Zuständig für die Vorabkontrolle ist der Beauftragte für den Datenschutz. Dieser nimmt die Vorabkontrolle nach Empfang der Übersicht nach § 4g Abs. 2 Satz 1 vor. Er hat sich in Zweifelsfällen an die Aufsichtsbehörde oder bei den Post- und Telekommunikationsunternehmen an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu wenden.

§ 4e Inhalt der Meldepflicht

Sofern Verfahren automatisierter Verarbeitungen meldepflichtig sind, sind folgende Angaben zu machen:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,

3. Anschrift der verantwortlichen Stelle,

4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,

5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,

6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,

7. Regelfristen für die Löschung der Daten,

8. eine geplante Datenübermittlung in Drittstaaten,

9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind. § 4d Abs. 1 und 4 gilt für die Änderung der nach Satz 1 mitgeteilten Angaben sowie für den Zeitpunkt der Aufnahme und der Beendigung der meldepflichtigen Tätigkeit entsprechend.

§ 4f Beauftragter für den Datenschutz

(1) Öffentliche und nicht öffentliche Stellen, die personenbezogene Daten automatisiert verarbeiten, haben einen Beauftragten für den Datenschutz schriftlich zu bestellen. Nicht-öffentliche Stellen sind hierzu spätestens innerhalb eines Monats nach Aufnahme ihrer Tätigkeit verpflichtet. Das Gleiche gilt, wenn personenbezogene Daten auf andere Weise erhoben, verarbeitet oder genutzt werden und damit in der Regel mindestens 20 Personen beschäftigt sind. Die Sätze 1 und 2 gelten nicht für die nichtöffentlichen Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Soweit aufgrund der Struktur einer öffentlichen Stelle erforderlich, genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche. Soweit nicht-öffentliche Stellen automatisierte Verarbeitungen vornehmen, die einer Vorabkontrolle unterliegen, oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung automatisiert verarbeiten, haben sie unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen Beauftragten für den Datenschutz zu bestellen.

(2) Zum Beauftragten für den Datenschutz darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Das Maß der erforderlichen Fachkunde bestimmt sich insbesondere nach dem Umfang der Datenverarbeitung der verantwortlichen Stelle und dem Schutzbedarf der personenbezogenen Daten, die die verantwortliche Stelle erhebt oder verwendet. Zum Beauftragten für den Datenschutz kann auch eine Person außerhalb der verantwortlichen Stelle bestellt werden; die Kontrolle erstreckt sich auch auf personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Öffentliche Stellen können mit Zustimmung ihrer Aufsichtsbehörde einen Bediensteten aus einer anderen öffentlichen Stelle zum Beauftragten für den Datenschutz bestellen.

(3) Der Beauftragte für den Datenschutz ist dem Leiter der öffentlichen oder nichtöffentlichen Stelle unmittelbar zu unterstellen. Er ist in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Die Bestellung zum Beauftragten für den Datenschutz kann in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuches, bei nicht-öffentlichen Stellen auch auf Verlangen der Aufsichtsbehörde, widerrufen werden. Ist nach Absatz 1 ein Beauftragter für den Datenschutz zu bestellen, so ist die Kündigung des Arbeitsverhältnisses unzulässig, es sei denn, dass Tatsachen vorliegen, welche die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigen. Nach der Abberufung als Beauftragter für den Datenschutz ist die Kündigung innerhalb eines Jahres nach der Beendigung der Bestellung unzulässig, es sei denn, dass die verantwortliche Stelle zur Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist berechtigt ist. Zur Erhaltung der zur Erfül-

lung seiner Aufgaben erforderlichen Fachkunde hat die verantwortliche Stelle dem Beauftragten für den Datenschutz die Teilnahme an Fort- und Weiterbildungsveranstaltungen zu ermöglichen und deren Kosten zu übernehmen.

(4) Der Beauftragte für den Datenschutz ist zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(4a) Soweit der Beauftragte für den Datenschutz bei seiner Tätigkeit Kenntnis von Daten erhält, für die dem Leiter oder einer bei der öffentlichen oder nichtöffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Beauftragten für den Datenschutz und dessen Hilfspersonal zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Beauftragten für den Datenschutz reicht, unterliegen seine Akten und andere Schriftstücke einem Beschlagnahmeverbot.

(5) Die öffentlichen und nicht-öffentlichen Stellen haben den Beauftragten für den Datenschutz bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Betroffene können sich jederzeit an den Beauftragten für den Datenschutz wenden.

§ 4g Aufgaben des Beauftragten für den Datenschutz

(1) Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin. Zu diesem Zweck kann sich der Beauftragte für den Datenschutz in Zweifelsfällen an die für die Datenschutzkontrolle bei der verantwortlichen Stelle zuständige Behörde wenden. Er kann die Beratung nach § 38 Abs. 1 Satz 2 in Anspruch nehmen. Er hat insbesondere

1. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen; zu diesem Zweck ist er über Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten,

2. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

(2) Dem Beauftragten für den Datenschutz ist von der verantwortlichen Stelle eine Übersicht über die in § 4e Satz 1 genannten Angaben sowie über zugriffsberechtigte Personen zur Verfügung zu stellen. Der Beauftragte für den Datenschutz macht die Angaben nach § 4e Satz 1 Nr. 1 bis 8 auf Antrag jedermann in geeigneter Weise verfügbar.

(2a) Soweit bei einer nichtöffentlichen Stelle keine Verpflichtung zur Bestellung eines Beauftragten für den Datenschutz besteht, hat der Leiter der nichtöffentlichen Stelle die Erfüllung der Aufgaben nach den Absätzen 1 und 2 in anderer Weise sicherzustellen.

(3) Auf die in § 6 Abs. 2 Satz 4 genannten Behörden findet Absatz 2 Satz 2 keine Anwendung. Absatz 1 Satz 2 findet mit der Maßgabe Anwendung, dass der behördliche Beauftragte für den Datenschutz das Benehmen mit dem Behördenleiter herstellt; bei Unstimmigkeiten zwischen dem behördlichen Beauftragten für den Datenschutz und dem Behördenleiter entscheidet die oberste Bundesbehörde.

§ 5 Datengeheimnis

Den bei der Datenverarbeitung beschäftigten Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind, soweit sie bei nicht-öffentlichen Stellen beschäftigt werden, bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 6 Rechte des Betroffenen

(1) Die Rechte des Betroffenen auf Auskunft (§§ 19, 34) und auf Berichtigung, Löschung oder Sperrung (§§ 20, 35) können nicht durch Rechtsgeschäft ausgeschlossen oder beschränkt werden.

(2) Sind die Daten des Betroffenen automatisiert in der Weise gespeichert, dass mehrere Stellen speicherungsberechtigt sind, und ist der Betroffene nicht in der Lage festzustellen, welche Stelle die Daten gespeichert hat, so kann er sich an jede dieser Stellen wenden. Diese ist verpflichtet, das Vorbringen des Betroffenen an die Stelle, die die Daten gespeichert hat, weiterzuleiten. Der Betroffene ist über die Weiterleitung und jene Stelle zu unterrichten. Die in § 19 Abs. 3 genannten Stellen, die Behörden der Staatsanwaltschaft und der Polizei sowie öffentliche Stellen der Finanzverwaltung, soweit sie personenbezogene Daten in Erfüllung ihrer gesetzlichen Aufgaben im Anwendungsbereich der Abgabenordnung zur Überwachung und Prüfung speichern, können statt des Betroffenen den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterrichten. In diesem Fall richtet sich das weitere Verfahren nach § 19 Abs. 6.

(3) Personenbezogene Daten über die Ausübung eines Rechts des Betroffenen, das sich aus diesem Gesetz oder aus einer anderen Vorschrift über den Datenschutz ergibt, dürfen nur zur Erfüllung der sich aus der Ausübung des Rechts ergebenden Pflichten der verantwortlichen Stelle verwendet werden.

§ 6a Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung liegt insbesondere dann vor, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder

2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

§ 6b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke

erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,

2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 19, 20, 34 und 35 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

§ 7 Schadensersatz

Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betrof-

fenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet.

(2) Bei einer schweren Verletzung des Persönlichkeitsrechts ist dem Betroffenen der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen.

(3) Die Ansprüche nach den Absätzen 1 und 2 sind insgesamt auf einen Betrag von 130.000 Euro begrenzt. Ist auf Grund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 130.000 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zu dem Höchstbetrag steht.

(4) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist der Geschädigte nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(5) Hat bei der Entstehung des Schadens ein Verschulden des Betroffenen mitgewirkt, gilt § 254 des Bürgerlichen Gesetzbuchs.

(6) Auf die Verjährung finden die für unerlaubte Handlungen geltenden Verjährungsvorschriften des Bürgerlichen Gesetzbuchs entsprechende Anwendung.

§ 9 Technische und organisatorische Maßnahmen

Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 9a Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

§ 10 Einrichtung automatisierter Abrufverfahren

(1) Die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dieses Verfahren unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen und der Aufgaben oder Geschäftszwecke der beteiligten Stellen angemessen ist. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Die beteiligten Stellen haben zu gewährleisten, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann. Hierzu haben sie schriftlich festzulegen:

1. Anlass und Zweck des Abrufverfahrens,

2. Dritte, an die übermittelt wird,

3. Art der zu übermittelnden Daten,

4. nach § 9 erforderliche technische und organisatorische Maßnahmen.

Im öffentlichen Bereich können die erforderlichen Festlegungen auch durch die Fachaufsichtsbehörden getroffen werden.

(3) Über die Einrichtung von Abrufverfahren ist in Fällen, in denen die in § 12 Abs. 1 genannten Stellen beteiligt sind, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit unter Mitteilung der Festlegungen nach Absatz 2 zu unterrichten. Die Einrichtung von Abrufverfahren, bei denen die in § 6 Abs. 2 und in § 19 Abs. 3 genannten Stellen beteiligt sind, ist nur zulässig, wenn das für die speichernde und die abrufende Stelle jeweils zuständige Bundes- oder Landesministerium zugestimmt hat.

(4) Die Verantwortung für die Zulässigkeit des einzelnen Abrufs trägt der Dritte, an den übermittelt wird. Die speichernde Stelle prüft die Zulässigkeit der Abrufe nur, wenn dazu Anlass besteht. Die speichernde Stelle hat zu gewährleisten, dass die Übermittlung personenbezogener Daten zumindest durch geeignete Stichprobenverfahren festgestellt und überprüft werden kann. Wird ein Gesamtbestand personenbezogener Daten abgerufen oder übermittelt (Stapelverarbeitung), so bezieht sich die Gewährleistung der Feststellung und Überprüfung nur auf die Zulässigkeit des Abrufes oder der Übermittlung des Gesamtbestandes.

(5) Die Absätze 1 bis 4 gelten nicht für den Abruf allgemein zugänglicher Daten. Allgemein zugänglich sind Daten, die jedermann, sei es ohne oder nach vorheriger Anmeldung Zulassung oder Entrichtung eines Entgelts, nutzen kann.

§ 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,

2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,

3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,

4. die Berichtigung, Löschung und Sperrung von Daten,

5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,

7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,

8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,

10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags. Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,

b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist, die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,

2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

Zweiter Abschnitt
Datenverarbeitung der öffentlichen Stellen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 12 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes gelten für öffentliche Stellen des Bundes, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

(2) Soweit der Datenschutz nicht durch Landesgesetz geregelt ist, gelten die §§ 12 bis 16, 19 bis 20 auch für die öffentlichen Stellen der Länder, soweit sie

1. Bundesrecht ausführen und nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen oder

2. als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt.

(3) Für Landesbeauftragte für den Datenschutz gilt § 23 Abs. 4 entsprechend.

(4) Werden personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt, gelten § 28 Absatz 2 Nummer 2 und die §§ 32 bis 35 anstelle der §§ 13 bis 16 und 19 bis 20.

§ 13 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist.

(1a) Werden personenbezogene Daten statt beim Betroffenen bei einer nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, sonst auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(2) Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

1. eine Rechtsvorschrift dies vorsieht oder aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert,

2. der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat,

3. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

4. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

5. dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist,

6. dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist,

7. dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen,

8. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann oder

9. dies aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen erforderlich ist.

§ 14 Datenspeicherung, -veränderung und -nutzung

(1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind. Ist keine Erhebung vorausgegangen, dürfen die Daten nur für die Zwecke geändert oder genutzt werden, für die sie gespeichert worden sind.

(2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt,

2. der Betroffene eingewilligt hat,

3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,

4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

5. die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Zweckänderung offensichtlich überwiegt,

6. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,

7. es zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Strafen oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 des Strafgesetzbuchs oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Bußgeldentscheidungen
erforderlich ist,

8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

9. es zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Eine Verarbeitung oder Nutzung für andere Zwecke liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen für die verantwortliche Stelle dient. Das gilt auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken durch die verantwortliche Stelle, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen.

(4) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

(5) Das Speichern, Verändern oder Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für andere Zwecke ist nur zulässig, wenn

1. die Voraussetzungen vorliegen, die eine Erhebung nach § 13 Abs. 2 Nr. 1 bis 6 oder 9 zulassen würden oder

2. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das öffentliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänderung

erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann. Bei der Abwägung nach Satz 1 Nr. 2 ist im Rahmen des öffentlichen Interesses das wissenschaftliche Interesse an dem Forschungsvorhaben besonders zu berücksichtigen.

(6) Die Speicherung, Veränderung oder Nutzung von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) zu den in § 13 Abs. 2 Nr. 7 genannten Zwecken richtet sich nach den für die in § 13 Abs. 2 Nr. 7 genannten Personen geltenden Geheimhaltungspflichten.

§ 15 Datenübermittlung an öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und

2. die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht. § 10 Abs. 4 bleibt unberührt.

(3) Der Dritte, an den die Daten übermittelt werden, darf diese für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 14 Abs. 2 zulässig.

(4) Für die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgesellschaften gelten die Absätze 1 bis 3 entsprechend, sofern sichergestellt ist, dass bei diesen ausreichende Datenschutzmaßnahmen getroffen werden.

(5) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen oder eines Dritten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder eines Dritten an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.
(6) Absatz 5 gilt entsprechend, wenn personenbezogene Daten innerhalb einer öffentlichen Stelle weitergegeben werden.

§ 16 Datenübermittlung an nicht-öffentliche Stellen

(1) Die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Nutzung nach § 14 zulassen würden, oder

2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. Das Übermitteln von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist abweichend von Satz 1 Nr. 2 nur zulässig, wenn die Voraussetzungen vorliegen, die eine Nutzung nach § 14 Abs. 5 und 6 zulassen würden oder soweit dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist.

(2) Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

(3) In den Fällen der Übermittlung nach Absatz 1 Nr. 2 unterrichtet die übermittelnde Stelle den Betroffenen von der Übermittlung seiner Daten. Dies gilt nicht, wenn damit zu rechnen ist, dass er davon auf andere Weise Kenntnis erlangt, oder wenn die Unterrichtung die öffentliche Sicherheit gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde.

(4) Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Die übermittelnde Stelle hat ihn darauf hinzuweisen. Eine Verarbeitung oder Nutzung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Absatz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

§ 17

(weggefallen)

§ 18 Durchführung des Datenschutzes in der Bundesverwaltung

(1) Die obersten Bundesbehörden, der Präsident des Bundeseisenbahnvermögens sowie die bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts, über die von der Bundesregierung oder einer obersten Bundesbehörde lediglich die Rechtsaufsicht ausgeübt wird, haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Das Gleiche gilt für die Vorstände der aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange diesen ein ausschließliches Recht nach dem Postgesetz zusteht.

(2) Die öffentlichen Stellen führen ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen. Für ihre automatisierten Verarbeitungen haben sie die An-

gaben nach § 4e sowie die Rechtsgrundlage der Verarbeitung schriftlich festzulegen. Bei allgemeinen Verwaltungszwecken dienenden automatisierten Verarbeitungen, bei welchen das Auskunftsrecht des Betroffenen nicht nach § 19 Abs. 3 oder 4 eingeschränkt wird, kann hiervon abgesehen werden. Für automatisierte Verarbeitungen, die in gleicher oder ähnlicher Weise mehrfach geführt werden, können die Festlegungen zusammengefasst werden.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 19 Auskunft an den Betroffenen

(1) Dem Betroffenen ist auf Antrag Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft
dieser Daten beziehen,

2. die Empfänger oder Kategorien von Empfängern, an die die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

In dem Antrag soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnet werden. Sind die personenbezogenen Daten weder automatisiert noch in nicht automatisierten Dateien gespeichert, wird die Auskunft nur erteilt, soweit der Betroffene Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht außer Verhältnis zu dem vom Betroffenen geltend gemachten Informationsinteresse steht. Die verantwortliche Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung, nach pflichtgemäßem Ermessen.

(2) Absatz 1 gilt nicht für personenbezogene Daten, die nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschließlich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde.

(3) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an Verfassungsschutzbehörden, den Bundesnachrichtendienst, den Militärischen Abschirmdienst und, soweit die Sicherheit des Bundes berührt wird, andere Behörden des Bundesministeriums der Verteidigung, ist sie nur mit Zustimmung dieser Stellen zulässig.

(4) Die Auskunftserteilung unterbleibt, soweit

1. die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben gefährden würde,

2. die Auskunft die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde oder

3. die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen und deswegen das Interesse des Betroffenen an der Auskunftserteilung zurücktreten muss.

(5) Die Ablehnung der Auskunftserteilung bedarf einer Begründung nicht, soweit durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden kann.

(6) Wird dem Betroffenen keine Auskunft erteilt, so ist sie auf sein Verlangen dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu erteilen, soweit nicht die jeweils zuständige oberste Bundesbehörde im Einzelfall feststellt, dass dadurch die Sicherheit des Bundes oder eines Landes gefährdet würde. Die Mitteilung des Bundesbeauftragten an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand der verantwortlichen Stelle zulassen, sofern diese nicht einer weitergehenden Auskunft zustimmt.

(7) Die Auskunft ist unentgeltlich.

§ 19a Benachrichtigung

(1) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er von der Speicherung, der Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

3. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist. Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 2 oder 3 abgesehen wird. (3) § 19 Abs. 2 bis 4 gilt entsprechend.

§ 20 Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten, die weder automatisiert verarbeitet noch in nicht automatisierten Dateien gespeichert sind, unrichtig sind, oder wird ihre Richtigkeit von dem Betroffenen bestritten, so ist dies in geeigneter Weise festzuhalten.

(2) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind zu löschen, wenn

1. ihre Speicherung unzulässig ist oder

2. ihre Kenntnis für die verantwortliche Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten, die automatisiert verarbeitet oder in nicht automatisierten Dateien gespeichert sind, sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die weder automatisiert verarbeitet noch in einer nicht automatisierten Datei gespeichert sind, sind zu sperren, wenn die Behörde im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen des Betroffenen beeinträchtigt würden und die Daten für die Aufgabenerfüllung der Behörde nicht mehr erforderlich sind.

(7) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerlässlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

(8) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(9) § 2 Abs. 1 bis 6, 8 und 9 des Bundesarchivgesetzes ist anzuwenden.

§ 21 Anrufung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Jedermann kann sich an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wenden, wenn er der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein. Für die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten durch Gerichte des Bundes gilt dies nur, soweit diese in Verwaltungsangelegenheiten tätig werden.

Dritter Unterabschnitt
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

§ 22 Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Deutsche Bundestag wählt auf Vorschlag der Bundesregierung den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit mit mehr als der Hälfte der gesetzlichen Zahl seiner Mitglieder. Der Bundesbeauftragte muss bei seiner Wahl das 35. Lebensjahr vollendet haben. Der Gewählte ist vom Bundespräsidenten zu ernennen.

(2) Der Bundesbeauftragte leistet vor dem Bundesminister des Innern folgenden Eid:

"Ich schwöre, dass ich meine Kraft dem Wohle des deutschen Volkes widmen, seinen Nutzen mehren, Schaden von ihm wenden, das Grundgesetz und die Gesetze des Bundes wahren und verteidigen, meine Pflichten gewissenhaft erfüllen und Gerechtigkeit gegen jedermann üben werde. So wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Bundesbeauftragten beträgt fünf Jahre. Einmalige Wiederwahl ist zulässig.

(4) Der Bundesbeauftragte steht nach Maßgabe dieses Gesetzes zum Bund in einem öffentlich-rechtlichen

Amtsverhältnis. Er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Rechtsaufsicht der Bundesregierung.

(5) Der Bundesbeauftragte wird beim Bundesministerium des Innern eingerichtet. Er untersteht der Dienstaufsicht des Bundesministeriums des Innern. Dem Bundesbeauftragten ist die für die Erfüllung seiner Aufgaben notwendige Personal- und Sachausstattung zur Verfügung zu stellen; sie ist im Einzelplan des Bundesministers des Innern in einem eigenen Kapitel auszuweisen. Die Stellen sind im Einvernehmen mit dem Bundesbeauftragten zu besetzen. Die Mitarbeiter können, falls sie mit der beabsichtigten Maßnahme nicht einverstanden sind, nur im Einvernehmen mit ihm versetzt,abgeordnet oder umgesetzt werden.

(6) Ist der Bundesbeauftragte vorübergehend an der Ausübung seines Amtes verhindert, kann der Bundesminister des Innern einen Vertreter mit der Wahrnehmung der Geschäfte beauftragen. Der Bundesbeauftragte soll dazu gehört werden.

§ 23 Rechtsstellung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Das Amtsverhältnis des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit beginnt mit der Aushändigung der Ernennungsurkunde. Es endet

1. mit Ablauf der Amtszeit,

2. mit der Entlassung.

Der Bundespräsident entlässt den Bundesbeauftragten, wenn dieser es verlangt oder auf Vorschlag der Bundesregierung, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen. Im Falle der Beendigung des Amtsverhältnisses erhält der Bundesbeauftragte eine vom Bundespräsidenten vollzogene Urkunde. Eine Entlassung wird mit der Aushändigung der Urkunde wirksam. Auf Ersuchen des Bundesministers des Innern ist der Bundesbeauftragte verpflichtet, die Geschäfte bis zur Ernennung seines Nachfolgers weiterzuführen.

(2) Der Bundesbeauftragte darf neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten abgeben.

(3) Der Bundesbeauftragte hat dem Bundesministerium des Innern Mitteilung über Geschenke zu machen, die er in Bezug auf sein Amt erhält. Das Bundesministerium des Innern entscheidet über die Verwendung der Geschenke.

(4) Der Bundesbeauftragte ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Bundesbeauftragter Tatsachen anvertraut haben, sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für die Mitarbeiter des Bundesbeauftragten mit der Maßgabe, daß über die Ausübung dieses Rechts der Bundesbeauftragte entscheidet. Soweit das Zeugnisverweigerungsrecht des Bundesbeauftragten reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Schriftstücken von ihm nicht gefordert werden.

(5) Der Bundesbeauftragte ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Bundesbeauftragte darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Bundesministeriums des Innern weder vor Gericht noch außergerichtlich aussagen oder Erklärungen abgeben. Unberührt bleibt die gesetzlich begründete Pflicht, Straftaten anzuzeigen und bei Gefährdung der freiheitlichen demokratischen Grundordnung für deren Erhaltung einzutreten. Für den Bundesbeauftragten und seine Mitarbeiter gelten die §§ 93, 97, 105 Abs. 1, § 111 Abs. 5 in Verbindung mit § 105 Abs. 1 sowie § 116 Abs. 1 der Abgabenordnung nicht. Satz 5 findet keine Anwendung, soweit die Finanzbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt der Bundesbeauftragte einen Datenschutzverstoß fest, ist er befugt, diesen anzuzeigen und den Betroffenen hierüber zu informieren.

(6) Die Genehmigung, als Zeuge auszusagen, soll nur versagt werden, wenn die Aussage dem Wohle des Bundes oder eines deutschen Landes Nachteile bereiten oder die Erfüllung öffentlicher Aufgaben ernstlich gefährden oder erheblich erschweren würde. Die Genehmigung, ein Gutachten zu erstatten, kann versagt werden, wenn die Erstattung den dienstlichen Interessen Nachteile bereiten würde. § 28 des Bundesverfassungsgerichtsgesetzes bleibt unberührt.

(7) Der Bundesbeauftragte erhält vom Beginn des Kalendermonats an, in dem das Amtsverhältnis beginnt, bis zum Schluß des Kalendermonats, in dem das Amtsverhältnis endet, im Falle des Absatzes 1 Satz 6 bis zum Ende des Monats, in dem die Geschäftsführung endet, Amtsbezüge in Höhe der einem Bundesbeamten der Besoldungsgruppe B 9 zustehenden Besoldung. Das Bundesreisekostengesetz und das Bundesumzugskostengesetz sind entsprechend anzuwenden. Im Übrigen sind § 12 Abs 6 sowie die §§ 13 bis 20 und 21a Abs. 5 des Bundesministergesetzes mit den Maßgaben anzuwenden, dass an die Stelle der vierjährigen Amtszeit in § 15 Abs. 1 des Bundesministergesetzes eine Amtszeit von fünf Jahren und an die Stelle der Besoldungsgruppe B 11 in § 21a Abs. 5 des Bundesministergesetzes die Be-

soldungsgruppe B 9 tritt. Abweichend von Satz 3 in Verbindung mit den §§ 15 bis 17 und 21a Abs. 5 des Bundesministergesetzes berechnet sich das Ruhegehalt des Bundesbeauftragten unter Hinzurechnung der Amtszeit als ruhegehaltsfähige Dienstzeit in entsprechender Anwendung des Beamtenversorgungsgesetzes, wenn dies günstiger ist und der Bundesbeauftragte sich unmittelbar vor seiner Wahl zum Bundesbeauftragten als Beamter oder Richter mindestens in dem letzten gewöhnlich vor Erreichen der Besoldungsgruppe B 9 zu durchlaufenden Amt befunden hat.

(8) Absatz 5 Satz 5 bis 7 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 24 Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit kontrolliert bei den öffentlichen Stellen des Bundes die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz.

(2) Die Kontrolle des Bundesbeauftragten erstreckt sich auch auf

1. von öffentlichen Stellen des Bundes erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs, und

2. personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach § 30 der Abgabenordnung, unterliegen. Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Personenbezogene Daten, die der Kontrolle durch die Kommission nach § 15 des Artikel 10-Gesetzes unterliegen, unterliegen nicht der Kontrolle durch den Bundesbeauftragten, es sei denn, die Kommission ersucht den Bundesbeauftragten, die Einhaltung der Vorschriften über den Datenschutz bei bestimmten Vorgängen oder in bestimmten Bereichen zu kontrollieren und ausschließlich ihr darüber zu berichten. Der Kontrolle durch den Bundesbeauftragten unterliegen auch nicht personenbezogene Daten in Akten über die Sicherheitsüberprüfung, wenn der Betroffene der Kontrolle der auf ihn bezogenen Daten im Einzelfall gegenüber dem Bundesbeauftragten widerspricht.

(3) Die Bundesgerichte unterliegen der Kontrolle des Bundesbeauftragten nur, soweit sie in Verwaltungsangelegenheiten tätig werden.

(4) Die öffentlichen Stellen des Bundes sind verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen ist dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren, die im Zusammenhang mit der Kontrolle nach Absatz 1 stehen,

2. jederzeit Zutritt in alle Diensträume zu gewähren.

Die in § 6 Abs. 2 und § 19 Abs. 3 genannten Behörden gewähren die Unterstützung nur dem Bundesbeauftragten selbst und den von ihm schriftlich besonders Beauftragten. Satz 2 gilt für diese Behörden nicht, soweit die oberste Bundesbehörde im Einzelfall feststellt, dass die Auskunft oder Einsicht die Sicherheit des Bundes oder eines Landes gefährden würde.

(5) Der Bundesbeauftragte teilt das Ergebnis seiner Kontrolle der öffentlichen Stelle mit. Damit kann er Vorschläge zur Verbesserung des Datenschutzes, insbesondere zur Beseitigung von festgestellten Mängeln bei der Verarbeitung oder Nutzung personenbezogener Daten, verbinden. § 25 bleibt unberührt.

(6) Absatz 2 gilt entsprechend für die öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind.

§ 25 Beanstandungen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Stellt der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet er dies

1. bei der Bundesverwaltung gegenüber der zuständigen obersten Bundesbehörde,

2. beim Bundeseisenbahnvermögen gegenüber dem Präsidenten,

3. bei den aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz zusteht, gegenüber deren Vorständen,

4. bei den bundesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen von Satz 1 Nr. 4 unterrichtet der Bundesbeauftragte gleichzeitig die zuständige Aufsichtsbehörde.

(2) Der Bundesbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt.

(3) Die Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die aufgrund der Bean-

standung des Bundesbeauftragten getroffen worden sind. Die in Absatz 1 Satz 1 Nr. 4 genannten Stellen leiten der zuständigen Aufsichtsbehörde gleichzeitig eine Abschrift ihrer Stellungnahme an den Bundesbeauftragten zu.

§ 26 Weitere Aufgaben des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

(1) Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit erstattet dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht. Er unterrichtet den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes.

(2) Auf Anforderung des Deutschen Bundestages oder der Bundesregierung hat der Bundesbeauftragte Gutachten zu erstellen und Berichte zu erstatten. Auf Ersuchen des Deutschen Bundestages, des Petitionsausschusses, des Innenausschusses oder der Bundesregierung geht der Bundesbeauftragte ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen des Bundes nach. Der Bundesbeauftragte kann sich jederzeit an den Deutschen Bundestag wenden.

(3) Der Bundesbeauftragte kann der Bundesregierung und den in § 12 Abs. 1 genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten. Die in § 25 Abs. 1 Nr. 1 bis 4 genannten Stellen sind durch den Bundesbeauftragten zu unterrichten, wenn die Empfehlung oder Beratung sie nicht unmittelbar betrifft.

(4) Der Bundesbeauftragte wirkt auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 hin. § 38 Abs. 1 Satz 4 und 5 gilt entsprechend.

Dritter Abschnitt
Datenverarbeitung nicht-öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen

Erster Unterabschnitt
Rechtsgrundlagen der Datenverarbeitung

§ 27 Anwendungsbereich

(1) Die Vorschriften dieses Abschnittes finden Anwendung, soweit personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen verarbeitet, genutzt oder dafür erhoben werden oder die Daten in oder aus nicht automatisierten Dateien verarbeitet, genutzt oder dafür erhoben werden durch 1. nicht-öffentliche Stellen,
2. a) öffentliche Stellen des Bundes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen,
b) öffentliche Stellen der Länder, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist. Dies gilt nicht, wenn die Erhebung, Verarbeitung oder Nutzung der Daten ausschließlich für persönliche oder familiäre Tätigkeiten erfolgt. In den Fällen der Nummer 2 Buchstabe a gelten anstelle des § 38 die §§ 18, 21 und 24 bis 26.
(2) Die Vorschriften dieses Abschnittes gelten nicht für die Verarbeitung und Nutzung personenbezogener Daten außerhalb von nicht automatisierten Dateien, soweit es sich nicht um personenbezogene Daten handelt, die offensichtlich aus einer automatisierten Verarbeitung entnommen worden sind.

§ 28 Datenerhebung und -speicherung für eigene Geschäftszwecke

(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,

2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder

3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.

Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.

(2) Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig

1. unter den Voraussetzungen des Absatzes 1 Satz 1 Nummer 2 oder Nummer 3,

2. soweit es erforderlich ist,

a) zur Wahrung berechtigter Interessen eines Dritten oder

b) zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder

3. wenn es im Interesse einer Forschungseinrichtung zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Zweckänder-

ung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(3) Die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung ist zulässig, soweit der Betroffene eingewilligt hat und im Falle einer nicht schriftlich erteilten Einwilligung die verantwortliche Stelle nach Absatz 3a verfährt. Darüber hinaus ist die Verarbeitung oder Nutzung personenbezogener Daten zulässig, soweit es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf die Zugehörigkeit des Betroffenen zu dieser Personengruppe, seine Berufs-, Branchen- oder Geschäftsbezeichnung, seinen Namen, Titel, akademischen Grad, seine Anschrift und sein Geburtsjahr beschränken, und die Verarbeitung oder Nutzung erforderlich ist

1. für Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle, die diese Daten mit Ausnahme der Angaben zur Gruppenzugehörigkeit beim Betroffenen nach Absatz 1 Satz 1 Nummer 1 oder aus allgemein zugänglichen Adress-, Rufnummern-, Branchen- oder vergleichbaren Verzeichnissen erhoben hat,

2. für Zwecke der Werbung im Hinblick auf die berufliche Tätigkeit des Betroffenen und unter seiner beruflichen Anschrift oder

3. für Zwecke der Werbung für Spenden, die nach § 10b Absatz 1 und § 34g des Einkommensteuergesetzes steuerbegünstigt sind. Für Zwecke nach Satz 2 Nummer 1 darf die verantwortliche Stelle zu den dort genannten Daten weitere Daten hinzuspeichern. Zusammengefasste personenbezogene Daten nach Satz 2 dürfen auch dann für Zwecke der Werbung übermittelt werden, wenn die Übermittlung nach Maßgabe des § 34 Absatz 1a Satz 1 gespeichert wird; in diesem Fall muss die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgehen. Unabhängig vom Vorliegen der Voraussetzungen des Satzes 2 dürfen personenbezogene Daten für Zwecke der Werbung für fremde Angebote genutzt werden, wenn für den Betroffenen bei der Ansprache zum Zwecke der Werbung die für die Nutzung der Daten verantwortliche Stelle eindeutig erkennbar ist. Eine Verarbeitung oder Nutzung nach den Sätzen 2 bis 4 ist nur zulässig,soweit schutzwürdige Interessen des Betroffenen nicht entgegenstehen. Nach den Sätzen 1, 2 und 4 übermittelte Daten dürfen nur für den Zweck verarbeitet oder genutzt werden, für den sie übermittelt worden sind.

(3a) Wird die Einwilligung nach § 4a Absatz 1 Satz 3 in anderer Form als der Schriftform erteilt, hat die verantwortliche Stelle dem Betroffenen den Inhalt der Einwilligung schriftlich zu bestätigen, es sei denn, dass die Einwilligung elektronisch erklärt wird und die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie in drucktechnisch deutlicher Gestaltung besonders hervorzuheben.

(3b) Die verantwortliche Stelle darf den Abschluss eines Vertrags nicht von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

(4) Widerspricht der Betroffene bei der verantwortlichen Stelle der Verarbeitung oder Nutzung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Verarbeitung oder Nutzung für diese Zwecke unzulässig. Der Betroffene ist bei der Ansprache zum Zweck der Werbung oder der Markt- oder Meinungsforschung und in den Fällen des Absatzes 1 Satz 1 Nummer 1 auch bei Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses über die verantwortliche Stelle sowie über das Widerspruchsrecht nach Satz 1 zu unterrichten; soweit der Ansprechende personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat er auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann. Widerspricht der Betroffene bei dem Dritten, dem die Daten im Rahmen der Zwecke nach Absatz 3 übermittelt worden sind, der Verarbeitung oder Nutzung für Zwecke der Werbung oder der Markt- oder Meinungsforschung, hat dieser die Daten für diese Zwecke zu sperren. In den Fällen des Absatzes 1 Satz 1 Nummer 1 darf für den Widerspruch keine strengere Form verlangt werden als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses.

(5) Der Dritte, dem die Daten übermittelt worden sind, darf diese nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nicht-öffentlichen Stellen nur unter den Voraussetzungen der Absätze 2 und 3 und öffentlichen Stellen nur unter den Voraussetzungen des § 14 Abs. 2 erlaubt. Die übermittelnde Stelle hat ihn darauf hinzuweisen.

(6) Das Erheben, Verarbeiten und Nutzen von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) für eigene Geschäftszwecke ist zulässig, soweit nicht der Betroffene nach Maßgabe des § 4a Abs. 3 eingewilligt hat, wenn

1. dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben,

2. es sich um Daten handelt, die der Betroffene offenkundig öffentlich gemacht hat,

3. dies zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwür-

dige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung überwiegt, oder

4. dies zur Durchführung wissenschaftlicher Forschung erforderlich ist, das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung und Nutzung erheblich überwiegt und der Zweck der Forschung auf andere Weise nicht oder nur mit unverhältnismäßigem Aufwand erreicht werden kann.

(7) Das Erheben von besonderen Arten personenbezogener Daten (§ 3 Abs. 9) ist ferner zulässig, wenn dies zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen. Die Verarbeitung und Nutzung von Daten zu den in Satz 1 genannten Zwecken richtet sich nach den für die in Satz 1 genannten Personen geltenden Geheimhaltungspflichten. Werden zu einem in Satz 1 genannten Zweck Daten über die Gesundheit von Personen durch Angehörige eines anderen als in § 203 Abs. 1 und 3 des Strafgesetzbuches genannten Berufes, dessen Ausübung die Feststellung, Heilung oder Linderung von Krankheiten oder die Herstellung oder den Vertrieb von Hilfsmitteln mit sich bringt, erhoben, verarbeitet oder genutzt, ist dies nur unter den Voraussetzungen zulässig, unter denen ein Arzt selbst hierzu befugt wäre.

(8) Für einen anderen Zweck dürfen die besonderen Arten personenbezogener Daten (§ 3 Abs. 9) nur unter den Voraussetzungen des Absatzes 6 Nr. 1 bis 4 oder des Absatzes 7 Satz 1 übermittelt oder genutzt werden. Eine Übermittlung oder Nutzung ist auch zulässig, wenn dies zur Abwehr von erheblichen Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten von erheblicher Bedeutung erforderlich ist.

(9) Organisationen, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keinen Erwerbszweck verfolgen, dürfen besondere Arten personenbezogener Daten (§ 3 Abs. 9) erheben, verarbeiten oder nutzen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Dies gilt nur für personenbezogene Daten ihrer Mitglieder oder von Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßig Kontakte mit ihr unterhalten. Die Übermittlung dieser personenbezogenen Daten an Personen oder Stellen außerhalb der Organisation ist nur unter den Voraussetzungen des § 4a Abs. 3 zulässig. Absatz 2 Nummer 2 Buchstabe b gilt entsprechend.

§ 28a Datenübermittlung an Auskunfteien

(1) Die Übermittlung personenbezogener Daten über eine Forderung an Auskunfteien ist nur zulässig, soweit die geschuldete Leistung trotz Fälligkeit nicht erbracht worden ist, die Übermittlung zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist und

1. die Forderung durch ein rechtskräftiges oder für vorläufig vollstreckbar erklärtes Urteil festgestellt worden ist oder ein Schuldtitel nach § 794 der Zivilprozessordnung vorliegt,

2. die Forderung nach § 178 der Insolvenzordnung festgestellt und nicht vom Schuldner im Prüfungstermin bestritten worden ist,

3. der Betroffene die Forderung ausdrücklich anerkannt hat,

4. a) der Betroffene nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist,

b) zwischen der ersten Mahnung und der Übermittlung mindestens vier Wochen liegen,

c) die verantwortliche Stelle den Betroffenen rechtzeitig vor der Übermittlung der Angaben, jedoch frühestens bei der ersten Mahnung über die bevorstehende Übermittlung unterrichtet hat und

d) der Betroffene die Forderung nicht bestritten hat oder

5. das der Forderung zugrunde liegende Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und die verantwortliche Stelle den Betroffenen über die bevorstehende Übermittlung unterrichtet hat. Satz 1 gilt entsprechend, wenn die verantwortliche Stelle selbst die Daten nach § 29 verwendet.

(2) Zur zukünftigen Übermittlung nach § 29 Abs. 2 dürfen Kreditinstitute personenbezogene Daten über die Begründung, ordnungsgemäße Durchführung und Beendigung eines Vertragsverhältnisses betreffend ein Bankgeschäft nach § 1 Abs. 1 Satz 2 Nr. 2, 8 oder Nr. 9 des Kreditwesengesetzes an Auskunfteien übermitteln, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Übermittlung gegenüber dem Interesse der Auskunftei an der Kenntnis der Daten offensichtlich überwiegt. Der Betroffene ist vor Abschluss des Vertrages hierüber zu unterrichten. Satz 1 gilt nicht für Giroverträge, die die Einrichtung eines Kontos ohne Überziehungsmöglichkeit zum Gegenstand haben. Zur zukünftigen Übermittlung nach § 29 Abs. 2 ist die Übermittlung von Daten über Verhaltensweisen des Betroffenen, die im Rahmen eines vorvertraglichen Vertrauensverhältnisses der Herstellung von Markttransparenz dienen, an Auskunfteien auch mit Einwilligung des Betroffenen unzulässig.

(3) Nachträgliche Änderungen der einer Übermittlung nach Absatz 1 oder Absatz 2 zugrunde liegenden Tatsachen hat die verantwortliche Stelle der Auskunftei innerhalb von einem Monat nach Kenntniserlangung mitzuteilen, solange die ursprünglich übermittelten Daten bei der Auskunftei gespeichert sind. Die Aus-

kunftei hat die übermittelnde Stelle über die Löschung der ursprünglich übermittelten Daten zu unterrichten.

§ 28b Scoring

Zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dem Betroffenen darf ein Wahrscheinlichkeitswert für ein bestimmtes zukünftiges Verhalten des Betroffenen erhoben oder verwendet werden, wenn

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind,

2. im Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 vorliegen,

3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschließlich Anschriftendaten genutzt werden,

4. im Fall der Nutzung von Anschriftendaten der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

§ 29 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

(1) Das geschäftsmäßige Erheben, Speichern, Verändern oder Nutzen personenbezogener Daten zum Zweck der Übermittlung, insbesondere wenn dies der Werbung, der Tätigkeit von Auskunfteien oder dem Adresshandel dient, ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Speicherung oder Veränderung hat,

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Speicherung oder Veränderung offensichtlich überwiegt, oder

3. die Voraussetzungen des § 28a Abs. 1 oder Abs. 2 erfüllt sind; Daten im Sinne von § 28a Abs. 2 Satz 4 dürfen nicht erhoben oder gespeichert werden. § 28 Absatz 1 Satz 2 und Absatz 3 bis 3b ist anzuwenden.

(2) Die Übermittlung im Rahmen der Zwecke nach Absatz 1 ist zulässig, wenn

1. der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und

2. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat. § 28 Absatz 3 bis 3b gilt entsprechend. Bei der Übermittlung nach Satz 1 Nr. 1 sind die Gründe für das Vorliegen eines berechtigten Interesses und die Art und Weise ihrer glaubhaften Darlegung von der übermittelnden Stelle aufzuzeichnen. Bei der Übermittlung im automatisierten Abrufverfahren obliegt die Aufzeichnungspflicht dem Dritten, dem die Daten übermittelt werden. Die übermittelnde Stelle hat Stichprobenverfahren nach § 10 Abs. 4 Satz 3 durchzuführen und dabei auch das Vorliegen eines berechtigten Interesses einzelfallbezogen festzustellen und zu überprüfen.

(3) Die Aufnahme personenbezogener Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse hat zu unterbleiben, wenn der entgegenstehende Wille des Betroffenen aus dem zugrunde liegenden elektronischen oder gedruckten Verzeichnis oder Register ersichtlich ist. Der Empfänger der Daten hat sicherzustellen, dass Kennzeichnungen aus elektronischen oder gedruckten Verzeichnissen oder Registern bei der Übernahme in Verzeichnisse oder Register übernommen werden.

(4) Für die Verarbeitung oder Nutzung der übermittelten Daten gilt § 28 Abs. 4 und 5.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

(6) Eine Stelle, die geschäftsmäßig personenbezogene Daten, die zur Bewertung der Kreditwürdigkeit von Verbrauchern genutzt werden dürfen, zum Zweck der Übermittlung erhebt, speichert oder verändert, hat Auskunftsverlangen von Darlehensgebern aus anderen Mitgliedstaaten der Europäischen Union oder anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum genauso zu behandeln wie Auskunftsverlangen inländischer Darlehensgeber.

(7) Wer den Abschluss eines Verbraucherdarlehensvertrags oder eines Vertrags über eine entgeltliche Finanzierungshilfe mit einem Verbraucher infolge einer Auskunft einer Stelle im Sinne des Absatzes 6 ablehnt, hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten. Die Unterrichtung unterbleibt, soweit hierdurch die öffentliche Sicherheit oder Ordnung gefährdet würde. § 6a bleibt unberührt.

§ 30 Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

(1) Werden personenbezogene Daten geschäftsmäßig erhoben und gespeichert, um sie in anonymisierter Form zu übermitteln, sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies

für die Erfüllung des Zwecks der Speicherung oder zu wissenschaftlichen Zwecken erforderlich ist.

(2) Die Veränderung personenbezogener Daten ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Veränderung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte, soweit nicht das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Veränderung offensichtlich überwiegt.

(3) Die personenbezogenen Daten sind zu löschen, wenn ihre Speicherung unzulässig ist.

(4) § 29 gilt nicht.

(5) § 28 Abs. 6 bis 9 gilt entsprechend.

§ 30a Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

(1) Das geschäftsmäßige Erheben, Verarbeiten oder Nutzen personenbezogener Daten für Zwecke der Markt- oder Meinungsforschung ist zulässig, wenn

1. kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder

2. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt. Besondere Arten personenbezogener Daten (§ 3 Absatz 9) dürfen nur für ein bestimmtes Forschungsvorhaben erhoben, verarbeitet oder genutzt werden.

(2) Für Zwecke der Markt- oder Meinungsforschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für diese Zwecke verarbeitet oder genutzt werden. Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf, dürfen nur für das Forschungsvorhaben verarbeitet oder genutzt werden, für das sie erhoben worden sind. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, wenn sie zuvor so anonymisiert werden, dass ein Personenbezug nicht mehr hergestellt werden kann.

(3) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens, für das die Daten erhoben worden sind, möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Diese Merkmale dürfen mit den Einzelangaben nur zusammengeführt werden, soweit dies nach dem Zweck des Forschungsvorhabens erforderlich ist.

(4) § 29 gilt nicht.

(5) § 28 Absatz 4 und 6 bis 9 gilt entsprechend.

§ 31 Besondere Zweckbindung

Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, dürfen nur für diese Zwecke verwendet werden.

§ 32 Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

(1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Zur Aufdeckung von Straftaten dürfen personenbezogene Daten eines Beschäftigten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, die Erhebung, Verarbeitung oder Nutzung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.

(2) Absatz 1 ist auch anzuwenden, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden, ohne dass sie automatisiert verarbeitet oder in oder aus einer nicht automatisierten Datei verarbeitet, genutzt oder für die Verarbeitung oder Nutzung in einer solchen Datei erhoben werden.

(3) Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

Zweiter Unterabschnitt
Rechte des Betroffenen

§ 33 Benachrichtigung des Betroffenen

(1) Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und der Identität der verantwortlichen Stelle zu benachrichtigen. Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, ist der Betroffene von der erstmaligen

Übermittlung und der Art der übermittelten Daten zu benachrichtigen. Der Betroffene ist in den Fällen der Sätze 1 und 2 auch über die Kategorien von Empfängern zu unterrichten, soweit er nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

(2) Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

2. die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheimgehalten werden müssen,

4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,

5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,

6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,

7. die Daten für eigene Zwecke gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

8. die Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

b) es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist,

9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist. Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Satz 1 Nr. 2 bis 7 abgesehen wird.

§ 34 Auskunft an den Betroffenen

(1) Die verantwortliche Stelle hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,

2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und

3. den Zweck der Speicherung.

Der Betroffene soll die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, ist Auskunft über die Herkunft und die Empfänger auch dann zu erteilen, wenn diese Angaben nicht gespeichert sind. Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(1a) Im Fall des § 28 Absatz 3 Satz 4 hat die übermittelnde Stelle die Herkunft der Daten und den Empfänger für die Dauer von zwei Jahren nach der Übermittlung zu speichern und dem Betroffenen auf Verlangen Auskunft über die Herkunft der Daten und den Empfänger zu erteilen. Satz 1 gilt entsprechend für den Empfänger.

(2) Im Fall des § 28b hat die für die Entscheidung verantwortliche Stelle dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte,

2. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten und

3. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die für die Entscheidung verantwortliche Stelle

1. die zur Berechnung der Wahrscheinlichkeitswerte genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder
2. bei einer anderen Stelle gespeicherte Daten nutzt.

Hat eine andere als die für die Entscheidung verantwortliche Stelle

1. den Wahrscheinlichkeitswert oder

2. einen Bestandteil des Wahrscheinlichkeitswerts berechnet, hat sie die insoweit zur Erfüllung der Auskunftsansprüche nach den Sätzen 1 und 2 erforderlichen Angaben auf Verlangen der für die Entscheidung verantwortlichen Stelle an diese zu übermitteln. Im Fall des Satzes 3 Nr. 1 hat die für die Entscheidung verantwortliche Stelle den Betroffenen zur Geltendmachung seiner Auskunftsansprüche unter Angabe des Namens und der Anschrift der anderen Stelle sowie der zur Bezeichnung des Einzelfalls notwendigen Angaben unverzüglich an diese zu verweisen, soweit sie die Auskunft nicht selbst erteilt. In diesem Fall hat die andere Stelle, die den Wahrscheinlichkeitswert berechnet hat, die Auskunftsansprüche nach den Sätzen 1 und 2 gegenüber dem Betroffenen unentgeltlich zu erfüllen. Die Pflicht der für die Berechnung des Wahrscheinlichkeitswerts verantwortlichen Stelle nach Satz 3 entfällt, soweit die für die Entscheidung verantwortliche Stelle von ihrem Recht nach Satz 4 Gebrauch macht.

(3) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung speichert, hat dem Betroffenen auf Verlangen Auskunft über die zu seiner Person gespeicherten Daten zu erteilen, auch wenn sie weder automatisiert verarbeitet werden noch in einer nicht automatisierten Datei gespeichert sind. Dem Betroffenen ist auch Auskunft zu erteilen über Daten, die

1. gegenwärtig noch keinen Personenbezug aufweisen, bei denen ein solcher aber im Zusammenhang mit der Auskunftserteilung von der verantwortlichen Stelle hergestellt werden soll,

2. die verantwortliche Stelle nicht speichert, aber zum Zweck der Auskunftserteilung nutzt.

Die Auskunft über die Herkunft und die Empfänger kann verweigert werden, soweit das Interesse an der Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsinteresse des Betroffenen überwiegt.

(4) Eine Stelle, die geschäftsmäßig personenbezogene Daten zum Zweck der Übermittlung erhebt, speichert oder verändert, hat dem Betroffenen auf Verlangen Auskunft zu erteilen über

1. die innerhalb der letzten zwölf Monate vor dem Zugang des Auskunftsverlangens übermittelten Wahrscheinlichkeitswerte für ein bestimmtes zukünftiges Verhalten des Betroffenen sowie die Namen und letztbekannten Anschriften der Dritten, an die die Werte übermittelt worden sind,

2. die Wahrscheinlichkeitswerte, die sich zum Zeitpunkt des Auskunftsverlangens nach den von der Stelle zur Berechnung angewandten Verfahren ergeben,

3. die zur Berechnung der Wahrscheinlichkeitswerte nach den Nummern 1 und 2 genutzten Datenarten sowie

4. das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form.

Satz 1 gilt entsprechend, wenn die verantwortliche Stelle

1. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten ohne Personenbezug speichert, den Personenbezug aber bei der Berechnung herstellt oder

2. bei einer anderen Stelle gespeicherte Daten nutzt.

(5) Die nach den Absätzen 1a bis 4 zum Zweck der Auskunftserteilung an den Betroffenen gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verwendet werden; für andere Zwecke sind sie zu sperren.

(6) Die Auskunft ist auf Verlangen in Textform zu erteilen, soweit nicht wegen der besonderen Umstände eine andere Form der Auskunftserteilung angemessen ist.

(7) Eine Pflicht zur Auskunftserteilung besteht nicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 nicht zu benachrichtigen ist.

(8) Die Auskunft ist unentgeltlich. Werden die personenbezogenen Daten geschäftsmäßig zum Zweck der Übermittlung gespeichert, kann der Betroffene einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform verlangen. Für jede weitere Auskunft kann ein Entgelt verlangt werden, wenn der Betroffene die Auskunft gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann. Das Entgelt darf über die durch die Auskunftserteilung entstandenen unmittelbar zurechenbaren Kosten nicht hinausgehen. Ein Entgelt kann nicht verlangt werden, wenn

1. besondere Umstände die Annahme rechtfertigen, dass Daten unrichtig oder unzulässig gespeichert werden, oder

2. die Auskunft ergibt, dass die Daten nach § 35 Abs. 1 zu berichtigen oder nach § 35 Abs. 2 Satz 2 Nr. 1 zu löschen sind.

(9) Ist die Auskunftserteilung nicht unentgeltlich, ist dem Betroffenen die Möglichkeit zu geben, sich im Rahmen seines Auskunftsanspruchs persönlich Kenntnis über die ihn betreffenden Daten zu verschaffen. Er ist hierauf hinzuweisen.

§ 35 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Geschätzte Daten sind als solche deutlich zu kennzeichnen.

(2) Personenbezogene Daten können außer in den Fällen des Absatzes 3 Nr. 1 und 2 jederzeit gelöscht werden. Personenbezogene Daten sind zu löschen, wenn

1. ihre Speicherung unzulässig ist,

2. es sich um Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, strafbare Handlungen oder Ordnungswidrigkeiten handelt und ihre Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann,

3. sie für eigene Zwecke verarbeitet werden, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist, oder

4. sie geschäftsmäßig zum Zweck der Übermittlung verarbeitet werden und eine Prüfung jeweils am Ende des vierten, soweit es sich um Daten über erledigte Sachverhalte handelt und der Betroffene der Löschung nicht widerspricht, am Ende des dritten Kalenderjahres beginnend mit dem Kalenderjahr, das der erstmaligen Speicherung folgt, ergibt, dass eine längerwährende Speicherung nicht erforderlich ist. Personenbezogene Daten, die auf der Grundlage von § 28a Abs. 2 Satz 1 oder § 29 Abs. 1 Satz 1 Nr. 3 gespeichert werden, sind nach Beendigung des Vertrages auch zu löschen, wenn der Betroffene dies verlangt.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit

1. im Fall des Absatzes 2 Satz 2 Nr. 3 einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten sind ferner zu sperren, soweit ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(4a) Die Tatsache der Sperrung darf nicht übermittelt werden.

(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Erhebung, Verarbeitung oder Nutzung überwiegt. Satz 1 gilt nicht, wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

(6) Personenbezogene Daten, die unrichtig sind oder deren Richtigkeit bestritten wird, müssen bei der geschäftsmäßigen Datenspeicherung zum Zweck der Übermittlung außer in den Fällen des Absatzes 2 Nr. 2 nicht berichtigt, gesperrt oder gelöscht werden, wenn sie aus allgemein zugänglichen Quellen entnommen und zu Dokumentationszwecken gespeichert sind. Auf Verlangen des Betroffenen ist diesen Daten für die Dauer der Speicherung seine Gegendarstellung beizufügen. Die Daten dürfen nicht ohne diese Gegendarstellung übermittelt werden.

(7) Von der Berichtigung unrichtiger Daten, der Sperrung bestrittener Daten sowie der Löschung oder Sperrung wegen Unzulässigkeit der Speicherung sind die Stellen zu verständigen, denen im Rahmen einer Datenübermittlung diese Daten zur Speicherung weitergegeben wurden, wenn dies keinen unverhältnismäßigen Aufwand erfordert und schutzwürdige Interessen des Betroffenen nicht entgegenstehen.

(8) Gesperrte Daten dürfen ohne Einwilligung des Betroffenen nur übermittelt oder genutzt werden, wenn

1. es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse der verantwortlichen Stelle oder eines Dritten liegenden Gründen unerläßlich ist und

2. die Daten hierfür übermittelt oder genutzt werden dürften, wenn sie nicht gesperrt wären.

Dritter Unterabschnitt
Aufsichtsbehörde

§§ 36 und 37

(weggefallen)

§ 38 Aufsichtsbehörde

(1) Die Aufsichtsbehörde kontrolliert die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz, soweit diese die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Dateien regeln einschließlich des Rechts der Mitgliedstaaten in den Fällen des § 1 Abs. 5. Sie berät und unterstützt die Beauftragten für den Datenschutz und die verantwortlichen Stellen mit Rücksicht auf deren typische Bedürfnisse. Die Aufsichtsbehörde darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten und nutzen; § 14 Abs. 2 Nr. 1 bis 3, 6 und 7 gilt entsprechend. Insbesondere darf die Aufsichtsbehörde zum Zweck der Aufsicht Daten an andere Aufsichtsbehörden übermitteln. Sie leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe). Stellt die Aufsichtsbehörde einen Verstoß gegen dieses Gesetz oder andere Vorschriften über den Datenschutz fest, so ist sie befugt, die Betroffenen hierüber zu unterrichten, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen sowie bei schwerwiegenden Verstößen die Gewerbeaufsichtsbehörde zur Durchführung gewerberechtlicher Maßnahmen zu unterricht-

en. Sie veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht. § 21 Satz 1 und § 23 Abs. 5 Satz 4 bis 7 gelten entsprechend.

(2) Die Aufsichtsbehörde führt ein Register der nach § 4d meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4e Satz 1. Das Register kann von jedem eingesehen werden. Das Einsichtsrecht erstreckt sich nicht auf die Angaben nach § 4e Satz 1 Nr. 9 sowie auf die Angabe der zugriffsberechtigten Personen.

(3) Die der Kontrolle unterliegenden Stellen sowie die mit deren Leitung beauftragten Personen haben der Aufsichtsbehörde auf Verlangen die für die Erfüllung ihrer Aufgaben erforderlichen Auskünfte unverzüglich zu erteilen. Der Auskunftspflichtige kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen der in § 383 Abs. 1 Nr. 1 bis 3 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem Gesetz über Ordnungswidrigkeiten aussetzen würde. Der Auskunftspflichtige ist darauf hinzuweisen.

(4) Die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen sind befugt, soweit es zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben erforderlich ist, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen. Sie können geschäftliche Unterlagen, insbesondere die Übersicht nach § 4g Abs. 2 Satz 1 sowie die gespeicherten personenbezogenen Daten und die Datenverarbeitungsprogramme, einsehen. § 24 Abs. 6 gilt entsprechend. Der Auskunftspflichtige hat diese Maßnahmen zu dulden.

(5) Zur Gewährleistung der Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz kann die Aufsichtsbehörde Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten oder technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen oder Mängeln, insbesondere solchen, die mit einer besonderen Gefährdung des Persönlichkeitsrechts verbunden sind, kann sie die Erhebung, Verarbeitung oder Nutzung oder den Einsatz einzelner Verfahren untersagen, wenn die Verstöße oder Mängel entgegen der Anordnung nach Satz 1 und trotz der Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt werden. Sie kann die Abberufung des Beauftragten für den Datenschutz verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit nicht besitzt.
(6) Die Landesregierungen oder die von ihnen ermächtigten Stellen bestimmen die für die Kontrolle der Durchführung des Datenschutzes im Anwendungsbereich dieses Abschnittes zuständigen Aufsichtsbehörden.

(7) Die Anwendung der Gewerbeordnung auf die den Vorschriften dieses Abschnittesunterliegenden Gewerbebetriebe bleibt unberührt.

§ 38a Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Vierter Abschnitt
Sondervorschriften

§ 39 Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

(1) Personenbezogene Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen und die von der zur Verschwiegenheit verpflichteten Stelle in Ausübung ihrer Berufs oder Amtspflicht zur Verfügung gestellt worden sind, dürfen von der verantwortlichen Stelle nur für den Zweck verarbeitet oder genutzt werden, für den sie sie erhalten hat. In die Übermittlung an eine nicht-öffentliche Stelle muss die zur Verschwiegenheit verpflichtete Stelle einwilligen.

(2) Für einen anderen Zweck dürfen die Daten nur verarbeitet oder genutzt werden, wenn die Änderung des Zwecks durch besonderes Gesetz zugelassen ist.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

(3) Die wissenschaftliche Forschung betreibenden Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

1. der Betroffene eingewilligt hat oder

2. dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

§ 41 Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

(1) Die Länder haben in ihrer Gesetzgebung vorzusehen, dass für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten von Unternehmen und Hilfsunternehmen der Presse ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken den Vorschriften der §§ 5, 9 und 38a entsprechende Regelungen einschließlich einer hierauf bezogenen Haftungsregelung entsprechend § 7 zur Anwendung kommen.

(2) Führt die journalistisch-redaktionelle Erhebung, Verarbeitung oder Nutzung personenbezogener Daten durch die Deutsche Welle zur Veröffentlichung von Gegendarstellungen des Betroffenen, so sind diese Gegendarstellungen zu den gespeicherten Daten zu nehmen und für dieselbe Zeitdauer aufzubewahren wie die Daten selbst.

(3) Wird jemand durch eine Berichterstattung der Deutschen Welle in seinem Persönlichkeitsrecht beeinträchtigt, so kann er Auskunft über die der Berichterstattung zugrunde liegenden, zu seiner Person gespeicherten Daten verlangen. Die Auskunft kann nach Abwägung der schutzwürdigen Interessen der Beteiligten verweigert werden, soweit

1. aus den Daten auf Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Rundfunksendungen berufsmäßig journalistisch mitwirken oder mitgewirkt haben, geschlossen werden kann,

2. aus den Daten auf die Person des Einsenders oder des Gewährsträgers von Beiträgen, Unterlagen und Mitteilungen für den redaktionellen Teil geschlossen werden kann,

3. durch die Mitteilung der recherchierten oder sonst erlangten Daten die journalistische Aufgabe der Deutschen Welle durch Ausforschung des Informationsbestandes beeinträchtigt würde. Der Betroffene kann die Berichtigung unrichtiger Daten verlangen.

(4) Im Übrigen gelten für die Deutsche Welle von den Vorschriften dieses Gesetzes die §§ 5, 7, 9 und 38a. Anstelle der §§ 24 bis 26 gilt § 42, auch soweit es sich um Verwaltungsangelegenheiten handelt.

§ 42 Datenschutzbeauftragter der Deutschen Welle

(1) Die Deutsche Welle bestellt einen Beauftragten für den Datenschutz, der an die Stelle des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit tritt. Die Bestellung erfolgt auf Vorschlag des Intendanten durch den Verwaltungsrat für die Dauer von vier Jahren, wobei Wiederbestellungen zulässig sind. Das Amt eines Beauftragten für den Datenschutz kann neben anderen Aufgaben innerhalb der Rundfunkanstalt wahrgenommen werden.

(2) Der Beauftragte für den Datenschutz kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz. Er ist in Ausübung dieses Amtes unabhängig und nur dem Gesetz unterworfen. Im Übrigen untersteht er der Dienst- und Rechtsaufsicht des Verwaltungsrates.

(3) Jedermann kann sich entsprechend § 21 Satz 1 an den Beauftragten für den Datenschutz wenden.

(4) Der Beauftragte für den Datenschutz erstattet den Organen der Deutschen Welle alle zwei Jahre, erstmals zum 1. Januar 1994 einen Tätigkeitsbericht. Er erstattet darüber hinaus besondere Berichte auf Beschluss eines Organes der Deutschen Welle. Die Tätigkeitsberichte übermittelt der Beauftragte auch an den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

(5) Weitere Regelungen entsprechend den §§ 23 bis 26 trifft die Deutsche Welle für ihren Bereich. Die §§ 4f und 4g bleiben unberührt.

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),

2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in

einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Fünfter Abschnitt
Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,

2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,

2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,

3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,

3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,

4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,

4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,

6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,

7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,

7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,

7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,

8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,

8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,

8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,

8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,

9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,

10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder

11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,

2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,

3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,

4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,

5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,

5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,

6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder

7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) Die Ordnungswidrigkeit kann im Fall des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.

§ 44 Strafvorschriften

(1) Wer eine in § 43 Abs. 2 bezeichnete vorsätzliche Handlung gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, begeht, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Sechster Abschnitt
Übergangsvorschriften

§ 45 Laufende Verwendungen

Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, sind binnen drei Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen. Soweit Vorschriften dieses Gesetzes in Rechtsvorschriften außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr zur Anwendung gelangen, sind Erhebungen, Verarbeitungen oder Nutzungen personenbezogener Daten, die am 23. Mai 2001 bereits begonnen haben, binnen fünf Jahren nach diesem Zeitpunkt mit den Vorschriften dieses Gesetzes in Übereinstimmung zu bringen.

§ 46 Weitergeltung von Begriffsbestimmungen

(1) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Datei verwendet, ist Datei

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht automatisierte Datei). Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(2) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Akte verwendet, ist Akte jede amtlichen oder dienstlichen Zwecken dienende Unterlage, die nicht dem Dateibegriff des Absatzes 1 unterfällt; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(3) Wird in besonderen Rechtsvorschriften des Bundes der Begriff Empfänger verwendet, ist Empfänger jede Person oder Stelle außerhalb der verantwortlichen Stelle. Empfänger sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen.

§ 47 Übergangsregelung

Für die Verarbeitung und Nutzung vor dem 1. September 2009 erhobener oder gespeicherter Daten ist § 28 in der bis dahin geltenden Fassung weiter anzuwenden

1. für Zwecke der Markt- oder Meinungsforschung bis zum 31. August 2010,

2. für Zwecke der Werbung bis zum 31. August 2012.

§ 48 Bericht der Bundesregierung

Die Bundesregierung berichtet dem Bundestag

1. bis zum 31. Dezember 2012 über die Auswirkungen der §§ 30a und 42a,

2. bis zum 31. Dezember 2014 über die Auswirkungen der Änderungen der §§ 28 und 29. Sofern sich aus Sicht der Bundesregierung gesetzgeberische Maßnahmen empfehlen, soll der Bericht einen Vorschlag enthalten.

Anlage (zu § 9 Satz 1)

(Fundstelle des Originaltextes: BGBl. I 2003, 88; bzgl. der einzelnen Änderungen vgl. Fußnote) Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),

2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),

3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),

4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),

5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),

8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.

Anhang 2: Berliner Datenschutzgesetz

Gesetz zum Schutz personenbezogener Daten in der Berliner Verwaltung (Berliner Datenschutzgesetz - BlnDSG) in der Fassung vom 17. Dezember 1990 (GVBl. 1991 S. 16, 54),
zuletzt geändert durch Gesetz vom 30. November 2007 (GVBl. S. 598)

Erster Abschnitt
Allgemeine Vorschriften

§ 1
Aufgabe und Gegenstand des Datenschutzes

(1) Aufgabe dieses Gesetzes ist es, die Verarbeitung personenbezogener Daten durch Behörden und sonstige öffentliche Stellen zu regeln, um

1. das Recht des einzelnen zu schützen, selbst über die Preisgabe und Verwendung seiner Daten zu bestimmen, soweit keine Einschränkungen in diesem Gesetz oder in anderen Rechtsvorschriften zugelassen sind (informationelles Selbstbestimmungsrecht),

2. die auf dem Grundsatz der Gewaltenteilung beruhende verfassungsmäßige Ordnung vor einer Gefährdung infolge der automatisierten Datenverarbeitung zu bewahren.

(2) Dieses Gesetz schützt personenbezogene Daten, die von Behörden oder sonstigen öffentlichen Stellen erhoben, gespeichert, verändert, übermittelt, gesperrt, gelöscht oder sonst genutzt werden.

§ 2
Anwendungsbereich

(1) Zum Schutz personenbezogener Daten nach Maßgabe dieses Gesetzes sind alle Behörden und sonstigen öffentlichen Stellen (insbesondere nichtrechtsfähige Anstalten, Krankenhausbetriebe, Eigenbetriebe und Gerichte) des Landes Berlin und der landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts (§ 28 des Allgemeinen Zuständigkeitsgesetzes) verpflichtet. Dies gilt auch für natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

(2) Betrifft die Datenverarbeitung frühere, bestehende oder künftige dienst- oder arbeitsrechtliche Rechtsverhältnisse, so gelten anstelle der §§ 9 bis 17 dieses Gesetzes § 28 Abs. 1 und 3 Nr. 1, §§ 31, 33 bis 35, 39 und 43 des Bundesdatenschutzgesetzes, soweit nichts anderes geregelt ist. Dies gilt auch für die Verarbeitung in Akten.

(3) Für öffentliche Stellen, die am Wettbewerb teilnehmen, gelten die §§ 3, 6, 6a, 9 bis 17 und 30 dieses Gesetzes nicht. Für sie gelten die §§ 11, 27 Abs. 2, §§ 28 bis 31, 33 bis 35, 39, 40 und 43 des Bundesdatenschutzgesetzes.

(4) Soweit personenbezogene Daten im Anwendungsbereich des Gesetzes über das Verfahren der Berliner Verwaltung verarbeitet werden, gelten die Vorschriften des Berliner Datenschutzgesetzes.

(5) Dieses Gesetz regelt den Schutz personenbezogener Daten für die Behörden und sonstigen öffentlichen Stellen umfassend. Andere Landesgesetze können für bestimmte Behörden und sonstige öffentliche Stellen einzelne notwendige Abweichungen von diesem Gesetz vorschreiben; im Übrigen richtet sich der Datenschutz auch in diesen Fällen nach den Vorschriften dieses Gesetzes.

§ 3
Verarbeitung personenbezogener Daten im Auftrag

(1) Die Vorschriften dieses Gesetzes gelten für die Behörden und sonstigen öffentlichen Stellen auch insoweit, als personenbezogene Daten in ihrem Auftrag durch andere Personen oder Stellen verarbeitet werden. In diesen Fällen ist der Auftragnehmer unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen (§ 5 Abs.1) sorgfältig auszuwählen. Der Auftrag ist unter Festlegung des Gegenstandes und des Umfangs der Datenverarbeitung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu erteilen. Der Auftraggeber hat sich von der Einhaltung der Maßnahmen nach Satz 3 zu überzeugen.

(2) Für die Behörden und sonstigen öffentlichen Stellen gelten die §§ 9 bis 17 dieses Gesetzes nicht, soweit sie personenbezogene Daten im Auftrag verarbeiten. In diesen Fällen ist die Verarbeitung personenbezogener Daten nur im Rahmen der Weisungen des Auftraggebers zulässig. Weisungen, die sich auf eine Datenverarbeitung richten, die gegen dieses Gesetz oder andere Rechtsvorschriften über den Datenschutz verstoßen, sind nicht auszuführen. Der Auftraggeber sowie dessen Aufsichtsbehörde sind unverzüglich zu unterrichten. Dasselbe gilt, wenn Daten verarbeitet werden sollen, die nach Ansicht des Auftragnehmers unter Verstoß gegen Rechtsvorschriften erlangt worden sind.

(3) Für juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, bei denen dem Land Berlin oder einer landesunmittelbaren Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht, gelten die Vorschriften des Vierten Abschnittes entsprechend, soweit sie in den Fällen des Absatzes 1 Satz 1 im Auftrag tätig werden. Hinsichtlich der Befugnisse nach § 28 Abs.1 wird das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes, Artikel 19 Abs. 2 Satz 1 der Verfassung von Berlin) für die Betriebs- und Geschäftszeit eingeschränkt.

(4) Sofern die Vorschriften dieses Gesetzes auf den Auftragnehmer keine Anwendung finden, ist der Auftraggeber verpflichtet, vertraglich sicherzustellen, dass der Auftragnehmer die Vorschriften dieses Gesetzes befolgt und sich, sofern die Datenverarbeitung im Geltungsbereich dieses Gesetzes durchgeführt wird, der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterwirft. Wird die Datenverarbeitung in einem anderen Bundesland oder in einem Mitgliedstaat der Europäischen Union durchgeführt, ist sicherzustellen, dass der Auftragnehmer einer Datenschutzkontrolle durch die jeweils zuständige Stelle unterliegt. Der Auftraggeber hat den Berliner Beauftragten für Datenschutz und Informationsfreiheit über die Beauftragung zu unterrichten.

§ 3a
Wartung

(1) Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat die datenverarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Dabei sind insbesondere folgende Anforderungen zu erfüllen: Es ist

1. sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt,

2. sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgen kann,

3. zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden,

4. sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können,

5. sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,

6. zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,

7. zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können, und

8. die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Eine Wartung durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur auf Grund schriftlicher Vereinbarungen erfolgen. Darin sind folgende Regelungen zu treffen:

1. Art und Umfang der Wartung,

2. Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer,

3. eine Protokollierungspflicht beim Auftraggeber und die Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,

4. die Daten dürfen ausschließlich für den Zweck der Wartung verwendet werden,

5. Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,

6. Löschung der Daten nach Abschluss der Wartungsarbeiten,

7. die technische Verbindung muss vom Auftraggeber hergestellt werden, sofern dies nicht möglich ist, ist ein Rückrufverfahren verbindlich festzulegen,

8. Anwesenheit des Systemverwalters ist möglichst sicherzustellen,

9. Verschlüsselung von personenbezogenen Daten auf dem Übertragungsweg nach dem jeweiligen Stand der Technik und

10. für den Fall, dass ein Auftragnehmer außerhalb der Mitgliedstaaten der Europäischen Union aus tätig wird, sind stets die jeweiligen Regelungen des § 14 über die Übermittlung personenbezogener Daten an ausländische und internationale Stellen anzuwenden. Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(3) Ist bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben, so dass die mit der Wartung betraute Stelle Betroffene nicht reidentifizieren kann, so sind nur Maßnahmen nach Absatz 2 Satz 1 und 3 erforderlich. Ein Zugriff darf nur zweckgebunden erfolgen.

(4) Im Sinne dieses Gesetzes ist

a) Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie die Überprüfung und Reparatur oder der Austausch von Hardware,

b) Fernwartung die Wartung der Hard- und Software von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung personenbezogener Daten erfolgt, mittels Einrichtung zur Datenübertragung vorgenommen wird, und

c) Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

§ 4
Begriffsbestimmungen

(1) Im Sinne dieses Gesetzes sind personenbezogene Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Entsprechendes gilt für Daten über Verstorbene, es sei denn, dass schutzwürdige Belange des Betroffenen nicht mehr beeinträchtigt werden können.

(2) Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen sowie Nutzen personenbezogener Daten. Im Sinne der nachfolgenden Vorschriften ist

1. Erheben das Beschaffen von Daten über den Betroffenen,

2. Speichern das Erfassen, Aufnehmen oder Aufbewahren von Daten auf einem Datenträger,

3. Verändern das inhaltliche Umgestalten gespeicherter Daten, ungeachtet der dabei angewendeten Verfahren,

4. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten in der Weise, dass die Daten durch die datenverarbeitende Stelle an den Dritten weitergegeben werden oder dass der Dritte zum Abruf bereitgehaltene Daten abruft,

5. Sperren das Verhindern weiterer Verarbeitung gespeicherter Daten,

6. Löschen das Beseitigen gespeicherter Daten,

7. Nutzen jede sonstige Verwendung personenbezogener Daten.

(3) Im Sinne dieses Gesetzes ist

1. datenverarbeitende Stelle jede Behörde oder sonstige öffentliche Stelle, die Daten für sich selbst verarbeitet oder durch andere verarbeiten lässt; nimmt diese unterschiedliche gesetzliche Aufgaben wahr, gilt diejenige Organisationseinheit als datenverarbeitende Stelle, der die Aufgabe zugewiesen ist,

2. Empfänger jede Person oder Stelle, die Daten erhält,

3. Dritter jede Person oder Stelle außerhalb der datenverarbeitenden Stelle, ausgenommen der Betroffene oder diejenigen Personen und Stellen, die in den Fällen der Nummer 1 im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union Daten im Auftrag verarbeitet,

4. automatisierte Datenverarbeitung jede durch Einsatz eines gesteuerten technischen Verfahrens selbständig ablaufende Datenverarbeitung,

5. eine Datei eine Sammlung von Daten, die durch automatisierte Verfahren ausgewertet werden kann (automatisierte Datei), oder eine gleichartig aufgebaute Sammlung von Daten, die nach bestimmten Merkmalen geordnet und ausgewertet werden kann (nicht automatisierte Datei),

6. eine Akte jede sonstigen amtlichen oder dienstlichen Zwecken dienende Unterlage, soweit sie nicht Datei im Sinne von Nummer 5 ist; dazu zählen auch Bild- und Tonträger, nicht jedoch Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen,

7. Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können,

8. Pseudonymisieren das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren.

9. mobiles personenbezogenes Speicher- und Verarbeitungsmedium ein Datenträger,

a) der an den Betroffenen ausgegeben wird,

b) auf dem personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und

c) bei dem der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

§ 5
Technische und organisatorische Maßnahmen

(1) Die Ausführungen der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz ist durch technische und organisatorische Maßnahmen sicherzustellen. Die Art und Weise der Maßnahmen hat für den angestrebten Schutzzweck angemessen zu sein und richtet sich nach dem jeweiligen Stand der Technik.

(2) Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),

2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben (Integrität),

3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können (Verfügbarkeit),

4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können (Authentizität),

5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit), und

6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können (Transparenz).

(3) Vor einer Entscheidung über den Einsatz oder eine wesentliche Änderung der automatisierten Datenverarbeitung sind die zu treffenden technischen und organisatorischen Maßnahmen auf der Grundlage einer Risikoanalyse und eines Sicherheitskonzepts zu ermitteln. Dazu gehört bei Verfahren, mit denen Daten verarbeitet werden, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen oder die zur Verfolgung von Straftaten und Ordnungswidrigkeiten erhoben werden, eine Vorabkontrolle hinsichtlich möglicher Gefahren für das Recht auf informationelle Selbstbestimmung. Entsprechend der technischen Entwicklung ist die Ermittlung in angemessenen Abständen zu wiederholen. Soweit trotz der realisierbaren Sicherheitsmaßnahmen untragbare Risiken verbleiben, die nicht durch Maßnahmen nach den Absätzen 1 und 2 oder eine Modifizierung der automatisierten Datenverarbeitung verhindert werden können, darf ein Verfahren nicht eingesetzt werden.

(4) Werden personenbezogene Daten nicht automatisiert verarbeitet, so findet Absatz 2 Nr. 1 bis 4 entsprechende Anwendung.

(5) Die automatisierte Datenverarbeitung soll so organisiert sein, dass bei der Verarbeitung, insbesondere der Übermittlung, der Kenntnisnahme im Rahmen der Aufgabenerfüllung und der Einsichtnahme, die Trennung der Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen möglich ist.

§ 5a
Datenvermeidung

Die Planung, Gestaltung und Auswahl informationstechnischer Produkte und Verfahren haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Zweiter Abschnitt
Voraussetzungen der Datenverarbeitung und Rechte der Betroffenen

§ 6
Zulässigkeit der Datenverarbeitung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn

1. dieses Gesetz oder

2. eine besondere Rechtsvorschrift sie erlaubt oder

3. der Betroffene eingewilligt hat.

Die Verarbeitung personenbezogener Daten ist nach diesem Gesetz zulässig, wenn wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Satz 1 Nr. 2 gilt nur, wenn die Rechtsvorschrift einen diesem Gesetz vergleichbaren Datenschutz gewährleistet.

(2) Werden aufgrund einer Rechtsvorschrift des Bundes personenbezogene Daten verarbeitet, ohne dass die Verarbeitung im Einzelnen geregelt ist, finden die §§ 13 bis 15 des Bundesdatenschutzgesetzes Anwendung.

(3) Wird die Datenverarbeitung auf die Einwilligung des Betroffenen gestützt, so ist dieser in geeigneter Weise über die Bedeutung der Einwilligung, insbesondere über den Verwendungszweck der Daten, aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten sowie den Zweck der Übermittlung. Der Betroffene ist unter Darlegung der Rechtsfolgen darauf hinzuweisen, dass er die Einwilligung verweigern kann.

(4) Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, so ist der Betroffene darauf schriftlich besonders hinzuweisen.

(5) Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf seiner freien Entscheidung beruht. Sie ist insbesondere unwirksam, wenn sie durch Androhung ungesetzlicher Nachteile oder durch fehlende Aufklärung bewirkt wurde. Soweit besondere Kategorien personenbezogener Daten nach § 6a Abs. 1 verarbeitet werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

(6) Die Einwilligung kann auch elektronisch erklärt werden. Es muss dabei sichergestellt werden, dass die Anforderungen zum Nachweis der Authentizität der Einwilligung jenen Anforderungen entsprechen, die für das zu Grunde liegende Verwaltungshandeln verlangt werden.

§ 6a
Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Personenbezogene Daten im Sinne des Artikels 8 Abs. 1 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG Nr. L 281 S. 31) – EG-Datenschutzrichtlinie –

dürfen nur verarbeitet werden, wenn angemessene Garantien zum Schutze des Rechtes auf informationelle Selbstbestimmung bestehen und eine besondere Rechtsvorschrift, die den Zweck der Verarbeitung bestimmt, dies erlaubt.

(2) Die Verarbeitung dieser Daten ist auch zulässig, wenn der Betroffene ausdrücklich eingewilligt hat oder die Verarbeitung zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist und der Betroffene aus rechtlichen oder tatsächlichen Gründen nicht in der Lage ist, seine Einwilligung zu geben.

(3) Die Absätze 1 und 2 finden keine Anwendung, wenn

1. Daten auf der Grundlage von § 2 Abs. 2 oder § 30 dieses Gesetzes verarbeitet werden oder

2. die Datenverarbeitung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist und die Verarbeitung dieser Daten durch ärztliches Personal oder durch sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen.

§ 7
Rechte des Betroffenen

Jeder hat nach Maßgabe dieses Gesetzes ein Recht auf

1. Auskunft, Benachrichtigung und Einsichtnahme (§ 16),

2. Berichtigung, Sperrung, Löschung und Widerspruch (§ 17),

3. Schadenersatz und Unterlassung (§ 18),

4. Einsicht in Beschreibungen und Verzeichnisse (§ 19a),

5. Anrufung des Berliner Beauftragten für Datenschutz und Informationsfreiheit (§ 27).

Auf diese Rechte kann der Betroffene nicht wirksam verzichten.

§ 8
Datengeheimnis

(1) Dienstkräften von Behörden und sonstigen öffentlichen Stellen, die Daten für sich oder im Auftrag verarbeiten, ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten. Diese Verpflichtung ist für Personen, die bei nicht öffentlichen Auftragnehmern öffentlicher Stellen dienstlichen Zugang zu personenbezogenen Daten haben, vertraglich sicherzustellen.

(2) Die Dienstkräfte sind bei der Aufnahme ihrer Tätigkeit nach Maßgabe des Absatzes 1 zu verpflichten. Ihre Pflichten bestehen auch nach Beendigung ihrer Tätigkeit fort.

§ 9
Erforderlichkeit

(1) Nach Maßgabe der nachfolgenden Vorschriften ist die Verarbeitung personenbezogener Daten nur zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der datenverarbeitenden Stelle zugewiesenen Aufgaben und für den jeweils damit verbundenen Zweck erforderlich ist.

(2) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach erforderlichen und nicht erforderlichen Daten auch durch Vervielfältigung und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist, so sind die Kenntnisnahme, die Weitergabe innerhalb der datenverarbeitenden Stelle und die Übermittlung der Daten, die nicht zur Erfüllung der jeweiligen Aufgabe erforderlich sind, über Absatz 1 hinaus zulässig. Diese Daten unterliegen insoweit einem Verwertungsverbot.

§ 10
Erheben

(1) Personenbezogene Daten sind unter der Voraussetzung des § 6 Abs. 1 und des § 6a Abs. 1 und 2 grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben.

(2) Werden Daten beim Betroffenen mit seiner Kenntnis erhoben, so ist er in geeigneter Weise über den Zweck der Datenerhebung aufzuklären. Die Aufklärungspflicht umfasst bei beabsichtigten Übermittlungen auch den Empfänger der Daten. Werden Daten bei dem Betroffenen auf Grund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, so ist er auf die Rechtsgrundlage hinzuweisen. Im Übrigen ist er darauf hinzuweisen, dass er die Auskunft verweigern kann. Sind die Angaben für die Gewährung einer Leistung erforderlich, so ist er über die möglichen Folgen einer Nichtbeantwortung aufzuklären.

(3) Bei Behörden und sonstigen öffentlichen Stellen dürfen Daten im Einzelfall ohne seine Kenntnis nur erhoben werden, wenn

1. eine Rechtsvorschrift dies erlaubt,

2. der Betroffene in diese Form der Erhebung eingewilligt hat oder

3. eine rechtzeitige Kenntnisgabe an den Betroffenen nicht möglich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Belange des Betroffenen beeinträchtigt werden könnten.

(4) Beim Betroffenen und bei Dritten außerhalb des öffentlichen Bereichs dürfen Daten ohne seine Kenntnis nur erhoben werden, wenn eine Rechtsvorschrift dieses vorsieht.

(5) Werden Daten ohne Kenntnis des Betroffenen erhoben, so ist er davon zu benachrichtigen, sobald die rechtmäßige Erfüllung der Aufgaben dadurch nicht mehr gefährdet wird. Die Benachrichtigung umfasst die Angabe der Rechtsgrundlage und die in Absatz 2 Satz 1 und 2 vorgesehene Aufklärung.

§ 11
Zweckbindung

(1) Personenbezogene Daten dürfen grundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind. Personenbezogene Daten, von denen eine Behörde oder sonstige öffentliche Stelle ohne Erhebung Kenntnis erlangt hat, dürfen nur für Zwecke genutzt werden, für die sie erstmals gespeichert worden sind.

(2) Sollen personenbezogene Daten zu Zwecken weiterverarbeitet werden, für die sie nicht erhoben oder gespeichert worden sind, so ist dies nur zulässig, wenn

1. eine der Voraussetzungen des § 6 Abs.1 oder des § 6a Abs. 1 oder 2 vorliegt,

2. es zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

3. sich bei Gelegenheit der rechtmäßigen Aufgabenerfüllung Anhaltspunkte für Straftaten oder Ordnungswidrigkeiten ergeben und die Unterrichtung der für die Verfolgung oder Vollstreckung zuständigen Behörden geboten erscheint. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der datenverarbeitenden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, findet Satz 1 Nr. 2 und 3 keine Anwendung.

(3) Sind personenbezogene Daten in Akten derart verbunden, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachen nicht oder nur mit unvertretbar großem Aufwand möglich ist, so tritt an die Stelle der Trennung ein Verwertungsverbot nach Maßgabe des Absatzes 2 für die Daten, die nicht dem Zweck der jeweiligen Verarbeitung dienen.

(4) Eine Verarbeitung zu anderen Zwecken liegt nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der internen Revision, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient. Der Zugriff auf personenbezogene Daten ist insoweit nur zulässig, als er für die Ausübung dieser Befugnisse unverzichtbar ist. Zu Aus- und Fortbildungszwecken dürfen personenbezogene Daten nur verwendet werden, wenn dies unerlässlich ist und schutzwürdige Belange des Betroffenen dem nicht entgegenstehen; zu Test- und Prüfungszwecken dürfen personenbezogene Daten nicht verwendet werden.

(5) Personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden, dürfen nicht für andere Zwecke verwendet werden.

§ 12
Datenübermittlung innerhalb des öffentlichen Bereichs

(1) Die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ist zulässig, wenn eine der Voraussetzungen des § 11 Abs. 2 Satz 1 Nr. 1 bis 3 vorliegt. Werden die Daten von einer Behörde oder sonstigen öffentlichen Stelle zur Erfüllung des gleichen Zwecks benötigt, zu dem die Daten erhoben worden sind, ist die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stellen ferner zulässig, wenn sie zur rechtmäßigen Erfüllung der durch Gesetz der übermittelnden Stelle oder der Behörde oder sonstigen öffentlichen Stelle zugewiesenen Aufgabe erforderlich ist.

(2) Die Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften ist in entsprechender Anwendung der Vorschriften über die Datenübermittlung an Behörden und sonstige öffentliche Stellen zulässig, sofern sichergestellt ist, dass bei dem Dritten hinreichende Datenschutzmaßnahmen getroffen werden.

(3) Über die Zulässigkeit der Datenübermittlung entscheidet die übermittelnde Stelle.

§ 13
Datenübermittlung an Stellen außerhalb des öffentlichen Bereichs

Die Übermittlung personenbezogener Daten an Personen und andere Stellen außerhalb des öffentlichen Bereichs sowie an landesunmittelbare Anstalten des öffentlichen Rechts, die am Wettbewerb teilnehmen, ist zulässig, wenn eine Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat.

§ 14
Datenübermittlung an öffentliche Stellen außerhalb des Geltungsbereichs des Grundgesetzes

(1) Für die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen im Geltungsbereich der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union gilt § 12 Abs. 1 entsprechend.

(2) Die Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union ist nur zulässig, soweit die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaft oder einer internationalen Vereinbarung ausdrücklich geregelt ist und wenn ein angemessenes Datenschutzniveau gewährleistet ist. Die Angemessenheit des Datenschutzniveaus ist von

der übermittelnden Stelle unter Berücksichtigung aller Umstände der beabsichtigten Datenübermittlung zu beurteilen, insbesondere nach der Art der Daten, ihrer Zweckbestimmung, der Dauer der geplanten Verarbeitung, dem Herkunfts- und dem Endbestimmungsland, den für den Empfänger geltenden Rechtsnormen sowie den für ihn geltenden Standesregeln und Sicherheitsmaßnahmen.

(3) Ist in den Fällen des Absatzes 2 kein angemessenes Datenschutzniveau gewährleistet, ist eine Übermittlung personenbezogener Daten zulässig, wenn

1. der Betroffene eingewilligt hat,

2. die Übermittlung für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich ist,

3. die Übermittlung für die Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist,

4. die Übermittlung aus einem Register erfolgt, das zur Information der Öffentlichkeit bestimmt ist oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind, oder

5. für die Übermittlung oder eine Kategorie von Übermittlungen insbesondere durch eine vertragliche Vereinbarung ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte sichergestellt werden. Die Stelle, an die die Daten übermittelt werden, ist auf die Zweckbindung nach § 11 Abs. 1 hinzuweisen.

(4) Die Senatsverwaltung für Inneres, der Berliner Beauftragte für Datenschutz und Informationsfreiheit und der behördliche Datenschutzbeauftragte sind über eine geplante Datenübermittlung nach den Absätzen 2 und 3 rechtzeitig zu unterrichten. Sie ist in der Dateibeschreibung nach § 19 Abs. 2 zu verzeichnen.

(5) Die Absätze 2 bis 4 finden keine Anwendung, soweit im Rahmen des internationalen Rechtshilfeverkehrs personenbezogene Daten übermittelt werden, die nicht automatisiert verarbeitet werden und auch nicht in Dateien gespeichert sind oder gespeichert werden sollen. In diesem Fall ist eine Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union zulässig, wenn

1. die Übermittlung in einem Gesetz, einem Rechtsakt der Europäischen Gemeinschaften oder einer internationalen Vereinbarung ausdrücklich geregelt ist oder

2. für den Empfänger gleichwertige Datenschutzregelungen gelten und bei einer Übermittlung an öffentliche Stellen die Voraussetzungen der §§ 9 und 11 erfüllt sind.

§ 15
Automatisiertes Abrufverfahren

(1) Ein automatisiertes Verfahren zum Abruf personenbezogener Daten durch Dritte darf durch Behörden oder sonstige öffentliche Stellen nur eingerichtet werden, wenn ein Gesetz dies ausdrücklich zulässt. Die Vorschriften über die Zulässigkeit des einzelnen Abrufs bleiben unberührt.

(2) Der Senat setzt durch Rechtsverordnung die Einzelheiten bei der Einrichtung automatisierter Abrufverfahren fest. Die Rechtsverordnung hat den Datenempfänger, die Datenart und den Zweck des Abrufs festzulegen. Sie hat Maßnahmen zur Datensicherung und zur Kontrolle vorzusehen, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen.

(3) Personenbezogene Daten dürfen für Stellen außerhalb des öffentlichen Bereichs zum automatisierten Abruf nicht bereitgehalten werden; dieses gilt nicht für den Betroffenen.

(4) Die Absätze 1 und 3 gelten nicht für Datenbestände, die jedermann ohne oder nach besonderer Zulassung zur Benutzung offen stehen oder deren Veröffentlichung zulässig wäre.

(5) Die Absätze 1, 2 und 4 sind auf die Zulassung regelmäßiger automatisierter Datenübermittlungen entsprechend anzuwenden.

§ 15a
Verbot automatisierter Einzelentscheidungen

Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Eine Entscheidung nach Satz 1 kann durch Gesetz zugelassen werden, wenn es die Wahrung der berechtigten Interessen des Betroffenen sicherstellt.

§ 16
Auskunft, Benachrichtigung und Einsichtnahme

(1) Werden personenbezogene Daten in einem automatisierten Verfahren oder in einer Datei gespeichert, so ist dem Betroffenen von der datenverarbeitenden Stelle auf Antrag gebührenfrei Auskunft zu erteilen über

1. die zu seiner Person gespeicherten Daten,

2. den Zweck und die Rechtsgrundlage der Verarbeitung,

3. die Herkunft der Daten und die Empfänger von Übermittlungen innerhalb der letzten zwei Jahre,

4. den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

(2) Werden personenbezogene Daten automatisiert verarbeitet, so ist der Betroffene von dieser Tatsache schriftlich zu benachrichtigen. Die Benachrichtigung umfasst einen Hinweis auf die Dateibeschreibung nach § 19 Abs. 2. Die Benachrichtigung kann zusammen mit der Erhebung erfolgen.

(3) Die Absätze 1 und 2 gelten nicht für personenbezogene Daten, die ausschließlich zum Zweck der Datensicherung gespeichert sind.

(4) Sind personenbezogene Daten in Akten gespeichert, so kann der Betroffene bei der datenverarbeitenden Stelle Einsicht in die Akten verlangen. Werden die Akten zur Person des Betroffenen geführt, so hat er sie zu bezeichnen. Werden die Akten nicht zur Person des Betroffenen geführt, so hat er Angaben zu machen, die das Auffinden der zu seiner Person gespeicherten Daten mit angemessenem Aufwand ermöglichen. Die Einsichtnahme ist unzulässig, wenn die Daten des Betroffenen mit Daten Dritter oder geheimhaltungsbedürftigen nicht personenbezogenen Daten derart verbunden sind, dass ihre Trennung nach verschiedenen Zwecken auch durch Vervielfältigen und Unkenntlichmachung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist; in diesem Fall ist dem Betroffenen Auskunft nach Absatz 1 zu erteilen. Im Übrigen kann mit Einwilligung des Betroffenen statt Einsicht Auskunft gewährt werden.

(5) Die Absätze 1, 2 und 4 gelten nicht, soweit eine Abwägung ergibt, dass die dort gewährten Rechte des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung oder einem überwiegenden Geheimhaltungsinteresse Dritter aus zwingenden Gründen zurücktreten müssen; die wesentlichen Gründe sind dem Betroffenen im Einzelnen mitzuteilen. Die Entscheidung trifft der Leiter der datenverarbeitenden Stelle oder dessen Stellvertreter. Werden Auskunft oder Einsicht nicht gewährt, so ist der Betroffene darauf hinzuweisen, dass er sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden kann. Die datenverarbeitende Stelle muss dem Berliner Beauftragten für Datenschutz und Informationsfreiheit die Gründe der Auskunfts- oder Einsichtsverweigerung darlegen.

§ 17
Berichtigung, Sperrung und Löschung von Daten, Widerspruchsrecht

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Der Betroffene ist vor der Berichtigung zu hören.

(2) Personenbezogene Daten sind zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und solange sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt. Sie sind ferner zu sperren, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Gesperrte Daten sind mit einem entsprechenden Vermerk zu versehen; sie dürfen nicht mehr verarbeitet, insbesondere übermittelt oder sonst genutzt werden, es sei denn, dass die Nutzung zu wissenschaftlichen Zwecken oder zur Behebung einer bestehenden Beweisnot unerlässlich ist und der Betroffene in die Nutzung eingewilligt hat.

(3) Personenbezogene Daten sind zu löschen, wenn ihre Kenntnis für die datenverarbeitende Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, dass durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Sie sind zu löschen, wenn ihre Speicherung unzulässig war oder wenn es in den Fällen des Absatzes 2 Satz 2 der Betroffene verlangt. In den Fällen des Satzes 2 1. Alternative ist der Betroffene vor der Löschung zu hören. Das gleiche gilt, wenn die Daten ohne Beteiligung des Betroffenen erhoben wurden und eine Benachrichtigung nach § 10 Abs. 5 nicht erfolgt ist.

(4) In den Fällen des Absatzes 2 Satz 2 und des Absatzes 3 Satz 1 und 2 kann die datenverarbeitende Stelle die Daten anstelle der dort vorgeschriebenen Sperrung oder Löschung einem dem öffentlichen Recht unterliegenden Archiv überantworten. Dazu ist die Einwilligung des Betroffenen in den Fällen des Absatzes 3 Satz 2 erforderlich.

(5) Von der Berichtigung nach Absatz 1, der Sperrung nach Absatz 2 und der Löschung nach Absatz 3 sind unverzüglich die Stellen zu verständigen, denen die Daten im Rahmen regelmäßiger Datenübermittlung übermittelt wurden.

(6) Sind personenbezogene Daten in Akten gespeichert und ist eine Sperrung nicht durch Vervielfältigen und Unkenntlichmachen möglich, so ist die Sperrung nach Absatz 2 Satz 1 nur durchzuführen, wenn die gesamte zur Person des Betroffenen geführte Akte zur Erfüllung der dort genannten Aufgaben nicht mehr erforderlich ist. Die Löschung nach Absatz 3 Satz 1 kann der Betroffene in diesem Fall nicht verlangen.

(7) Wenn der Betroffene schriftlich Widerspruch gegen die Datenverarbeitung einlegt und begründet, dass der rechtmäßigen Verarbeitung seiner Daten ein schutzwürdiges besonderes persönliches Interesse entgegensteht, ist die Verarbeitung der Daten nur zulässig, wenn im Einzelfall das öffentliche Interesse an der Datenverarbeitung gegenüber dem persönlichen Interesse des Betroffenen überwiegt; dem Betroffenen ist das Ergebnis der Abwägung mit Begründung schriftlich mitzuteilen.

§ 18
Schadenersatz- und Unterlassungsanspruch

(1) Wird der Betroffene durch eine nach diesem Gesetz oder anderen Rechtsvorschriften über den Datenschutz rechtswidrige Datenverarbeitung in seinen schutzwürdigen Belangen beeinträchtigt, so hat ihm

diejenige Behörde oder sonstige öffentliche Stelle, die die Daten
verarbeitet oder nach § 3 Abs.1 verarbeiten lässt, den daraus entstandenen Vermögensschaden zu ersetzen. Sind weitere Rechtsverletzungen zu besorgen, so kann der Betroffene Unterlassung verlangen. In schweren Fällen kann der Betroffene auch wegen des Schadens, der nicht Vermögensschaden ist, eine billige Entschädigung in Geld verlangen.

(2) Sind an einer automatisierten Bearbeitung mehrere Stellen beteiligt und lässt sich die speichernde Stelle nicht feststellen, so haftet jede dieser Stellen.

(3) Schadenersatz- und Unterlassungsansprüche auf Grund anderer Vorschriften bleiben unberührt.

§ 19
Durchführung des Datenschutzes und Dateibeschreibung

(1) Die datenverarbeitenden Stellen, in den Fällen des § 4 Abs. 3 Nr. 1 Halbsatz 2 auch die jeweiligen Behörden oder sonstigen öffentlichen Stellen, und die Aufsichtsbehörden haben für ihren Geschäftsbereich die Ausführung dieses Gesetzes sowie anderer Rechtsvorschriften über den Datenschutz sicherzustellen. Sie haben insbesondere dafür zu sorgen, dass die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, gewährleistet ist.

(2) Für automatisierte Verarbeitungen hat die datenverarbeitende Stelle schriftlich festzulegen:

1. Name und Anschrift der datenverarbeitenden Stelle,

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung,

3. Beschreibung der betroffenen Personengruppe und der diesbezüglichen Daten oder Datenkategorien,

4. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden,

5. Herkunft regelmäßig empfangener Daten,

6. zugriffsberechtigte Personen oder Personengruppen,

7. Fristen für die Sperrung und Löschung der Daten,

8. geplante Übermittlung personenbezogener Daten an Behörden oder sonstige öffentliche Stellen außerhalb des Geltungsbereichs der Rechtsvorschriften zum Schutz personenbezogener Daten der Mitgliedstaaten der Europäischen Union,

9. Betriebsart des Verfahrens, Art der Geräte, Stellen, bei denen sie aufgestellt sind, und das Verfahren zur Übermittlung, Sperrung, Löschung und Auskunftserteilung,

10. Beschreibung der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung (§ 5 Abs. 3 Satz 1),

11. Ergebnisse der Vorabkontrollen (§ 19a Abs. 1 Satz 3 Nr. 1).

(3) Absatz 2 findet keine Anwendung auf Dateien, die bei automatisierter Verarbeitung ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden.

§ 19a
Behördlicher Datenschutzbeauftragter

(1) Die Behörden und sonstigen öffentlichen Stellen haben Datenschutzbeauftragte (behördliche Datenschutzbeauftragte) sowie jeweils einen Vertreter schriftlich zu bestellen. Für mehrere Behörden oder sonstige öffentliche Stellen kann ein gemeinsamer Datenschutzbeauftragter bestellt werden. Die behördlichen Datenschutzbeauftragten haben insbesondere

1. bei den mit besonderen Risiken für Rechte und Freiheiten von Betroffenen verbundenen Verarbeitungen vor Beginn der Verarbeitung eine Prüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen nach § 5 durchzuführen (Vorabkontrolle),

2. die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen,

3. die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften dieses Gesetzes sowie anderen Vorschriften über den Datenschutz, bezogen auf die besonderen Verhältnisse in diesem Geschäftsbereich und die sich daraus ergebenen besonderen Erfordernisse für den Datenschutz, vertraut zu machen und

4. die Behörde oder sonstige öffentliche Stelle bei der Sicherstellung des Datenschutzes zu unterstützen; sie unterstützen auch die Personalvertretungen bei der Sicherstellung des Datenschutzes, soweit bei diesen personenbezogene Daten verarbeitet werden. Der behördliche Datenschutzbeauftragte führt die Beschreibungen und Verzeichnisse nach § 19. Diese können von jeder Person unentgeltlich eingesehen werden. Dies gilt nicht für die Angaben zu § 19 Abs. 2 Nr. 9 bis 11, soweit dadurch die Sicherheit des technischen Verfahrens beeinträchtigt wird. Dies gilt ferner nicht für Beschreibungen für Aufgaben des Verfassungsschutzes, der Gefahrenabwehr, der Strafverfolgung und der Steuerverwaltung, soweit die datenverarbeitende Stelle eine Einsichtnahme im Einzelfall mit der Erfüllung ihrer Aufgaben für unvereinbar erklärt, sowie für öffentliche Stellen, die am Wettbewerb teilnehmen.

(2) Zum behördlichen Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt und durch die Bestellung keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird. Er muss in einem Dienst- oder Arbeitsverhält-

nis bei einer Behörde oder sonstigen öffentlichen Stelle des Landes Berlin oder einer landesunmittelbaren Körperschaft, Anstalt oder Stiftung des öffentlichen Rechts stehen. Seine Bestellung kann gegen seinen Willen nur aus wichtigem Grund in entsprechender Anwendung von § 626 des Bürgerlichen Gesetzbuchs widerrufen werden. Er kann sich in Angelegenheiten des Datenschutzes unmittelbar an den Leiter der jeweiligen Behörde oder sonstigen öffentlichen Stelle wenden und unterliegt in Datenschutzangelegenheiten keinen Weisungen. Er darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden. Er ist zur Verschwiegenheit über die Identität Betroffener sowie über die Umstände, die Rückschlüsse auf Betroffene zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird.

(3) Der behördliche Datenschutzbeauftragte ist befugt, personenbezogene Daten zu verarbeiten, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Die jeweilige Behörde oder sonstige öffentliche Stelle hat den behördlichen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen und ihm insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen. Er ist über Vorhaben der automatisierten Verarbeitung rechtzeitig zu unterrichten.

(4) Der behördliche Datenschutzbeauftragte kann sich jederzeit an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden. In Zweifelsfällen der Vorabkontrolle ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit zu konsultieren.

Dritter Abschnitt
Daten für das Abgeordnetenhaus und die Bezirksverordnetenversammlungen

§ 20

(1) Die Behörden und sonstigen öffentlichen Stellen haben dem Abgeordnetenhaus, dessen verfassungsmäßigen Organen und den Fraktionen des Abgeordnetenhauses die von diesen im Rahmen ihrer Aufgaben verlangten Auskünfte über Daten zu erteilen. Personenbezogene Daten dürfen an diese Institutionen zur Erfüllung ihrer Aufgaben nur herausgegeben werden, wenn die in § 28 Abs. 3 Satz 1 Nr. 3 und Satz 2 des Bundesdatenschutzgesetzes genannten Voraussetzungen erfüllt sind.

(2) Dieselbe Verpflichtung besteht gegenüber den Bezirksverordnetenversammlungen, ihren verfassungsmäßigen Organen und ihren Fraktionen, soweit diese im Rahmen ihrer Zuständigkeiten Auskünfte über Daten verlangen.

(3) Gesetzesvorlagen müssen Angaben über die Daten, die für den Vollzug des Gesetzes mit Datenverarbeitungsanlagen erforderlich sind, und über die Form der vorgesehenen Datenverarbeitung enthalten.

Vierter Abschnitt
Berliner Beauftragter für Datenschutz und Informationsfreiheit

§ 21
Bestellung und Entlassung

(1) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit wird vom Abgeordnetenhaus mit den Stimmen der Mehrheit seiner Mitglieder gewählt und vom Präsidenten des Abgeordnetenhauses ernannt. Er nimmt zugleich die Aufgaben des Beauftragten für Akteneinsicht nach § 18 Abs. 1 des Berliner Informationsfreiheitsgesetzes vom 15. Oktober 1999 (GVBl. S. 561), das durch Artikel XXII des Gesetzes vom 16. Juli 2001 (GVBl. S. 260) geändert worden ist, wahr und führt die Amts- und Funktionsbezeichnung "Berliner Beauftragter für Datenschutz und Informationsfreiheit" in männlicher oder in weiblicher Form.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit leistet vor dem Präsidenten des Abgeordnetenhauses folgenden Eid:

"Ich schwöre, mein Amt gerecht und unparteiisch getreu dem Grundgesetz, der Verfassung von Berlin und den Gesetzen zu führen und meine ganze Kraft dafür einzusetzen, so wahr mir Gott helfe."

Der Eid kann auch ohne religiöse Beteuerung geleistet werden.

(3) Die Amtszeit des Berliner Beauftragten für Datenschutz und Informationsfreiheit beträgt fünf Jahre; nach dem Ende der Amtszeit bleibt er auf Aufforderung des Präsidiums des Abgeordnetenhauses bis zur Ernennung eines Nachfolgers im Amt. Die Wiederwahl ist zulässig. Vor Ablauf seiner Amtszeit kann der Berliner Beauftragte für Datenschutz und Informationsfreiheit gegen seinen Willen nur entlassen werden, wenn Gründe vorliegen, die bei einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen.

§ 22
Rechtsstellung

(1) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit steht nach Maßgabe dieses Gesetzes in einem öffentlich-rechtlichen Amtsverhältnis.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit wird als oberste Landesbehörde eingerichtet; er ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Präsidenten des Abgeordnetenhauses.

(3) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit darf neben seinem Amt kein weiteres besoldetes Amt und kein Gewerbe ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens noch einer Regierung oder einer gesetzgebenden Körperschaft des Bundes oder eines Landes angehören. Er darf nicht gegen Entgelt außergerichtliche Gutachten

abgeben. Seine Rechtsstellung wird im Übrigen durch Vertrag geregelt.

(4) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist berechtigt und kann von der Mehrheit des Abgeordnetenhauses oder eines Ausschusses verpflichtet werden, vor dem Parlament oder dem betreffenden Ausschuss zu erscheinen und zu reden. Er ist vor dem Erlass von den Datenschutz betreffenden Gesetzen, Rechtsverordnungen und Verwaltungsvorschriften anzuhören.

§ 23
Verschwiegenheitspflicht

Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist, auch nach Beendigung seines Amtsverhältnisses, verpflichtet, über die ihm amtlich bekannt gewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit darf, auch wenn er nicht mehr im Amt ist, über solche Angelegenheiten ohne Genehmigung des Präsidenten des Abgeordnetenhauses weder vor Gericht noch außergerichtlich Aussagen oder Erklärungen abgeben.

§ 24
Aufgaben und Befugnisse

(1) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit kontrolliert die Einhaltung der Vorschriften dieses Gesetzes sowie anderer Vorschriften über den Datenschutz bei den Behörden und sonstigen öffentlichen Stellen. Zu diesem Zweck kann er Empfehlungen zur Verbesserung des Datenschutzes geben; insbesondere kann er den Senat und einzelne Mitglieder des Senats sowie die übrigen Behörden und sonstigen öffentlichen Stellen in Fragen des Datenschutzes beraten. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist bei der Vorabkontrolle nach § 5 Abs. 3 zu beteiligen, wenn sie den beabsichtigten Einsatz verwaltungsübergreifender Verfahren betrifft. Er hat darüber hinaus die Befugnisse, die den für Datenschutz zuständigen Aufsichts- und Kontrollbehörden durch internationale oder europäische Rechtsakte zugewiesen werden.

(2) Ausgenommen von Absatz 1 sind die Gerichte, soweit sie nicht in Verwaltungsangelegenheiten tätig werden. Setzen Gerichte zur Erfüllung ihrer gesetzlichen Aufgaben automatische Datenverarbeitungsanlagen ein, so unterliegt unbeschadet der richterlichen Unabhängigkeit die Ordnungsmäßigkeit und Rechtmäßigkeit der Verfahren der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit.

(3) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit beobachtet die Auswirkungen der automatischen Datenverarbeitung auf die Arbeitsweise und die Entscheidungsbefugnisse der Behörden und sonstigen öffentlichen Stellen dahingehend, ob sie zu einer Beschränkung der Kontrollmöglichkeiten durch das Abgeordnetenhaus oder die Bezirksverordnetenversammlungen führen. Er kann Maßnahmen zum Schutz gegen derartige Auswirkungen anregen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist über die Einführung neuer Automationsvorhaben und wesentliche Änderungen automatisierter Datenverarbeitungen im Bereich der Behörden und sonstigen öffentlichen Stellen zu informieren.

(4) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit arbeitet mit den Behörden und sonstigen öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, und mit den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes zusammen. Er ist berechtigt, an diese Stellen personenbezogene Daten zu übermitteln, soweit dies zur Kontrolle der Einhaltung datenschutzrechtlicher Vorschriften erforderlich ist. Er ist ferner berechtigt, für diese Stellen auf ihr Ersuchen die Einhaltung datenschutzrechtlicher Vorschriften zu kontrollieren und in diesem Zusammenhang personenbezogene Daten zu erheben und sie an diese Stellen zu übermitteln; dies gilt auch, wenn sich eine nicht öffentliche Stelle durch Vertrag seiner Kontrolle unterworfen hat. Er leistet den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe (Amtshilfe).

(5) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist befugt, personenbezogene Daten, die ihm durch Beschwerden, Anfragen, Hinweise und Beratungsersuchen bekannt werden, zu verarbeiten, soweit dies zur Erfüllung seiner Aufgaben nach diesem Gesetz und dem Bundesdatenschutzgesetz erforderlich ist. Er darf im Rahmen von Kontrollmaßnahmen im Einzelfall personenbezogene Daten auch ohne Kenntnis des Betroffenen erheben, wenn nur auf diese Weise festgestellt werden kann, ob ein datenschutzrechtlicher Mangel besteht. Die nach den Sätzen 1 und 2 erhobenen und verarbeiteten Daten dürfen nicht zu anderen Zwecken weiterverarbeitet werden. Soweit der Berliner Beauftragte für Datenschutz und Informationsfreiheit von seinem Strafantragsrecht nach § 32 Abs.3 Gebrauch macht, ist er befugt, der Staatsanwaltschaft personenbezogene Daten zu übermitteln, soweit dies zur Durchführung des Ermittlungsverfahrens erforderlich ist.

§ 25
Dateienregister

(aufgehoben)

§ 26
Beanstandungen

(1) Stellt der Berliner Beauftragte für Datenschutz und Informationsfreiheit Verstöße gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dies

1. bei Behörden und sonstigen öffentlichen Stellen der Hauptverwaltung gegenüber dem zuständigen Mitglied

des Senats, im Übrigen gegenüber dem Präsidenten des Abgeordnetenhauses oder dem Präsidenten des Rechnungshofes,

2. bei Behörden und sonstigen öffentlichen Stellen der Bezirksverwaltungen gegenüber den Bezirksämtern,

3. bei den landesunmittelbaren Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie bei Vereinigungen solcher Körperschaften, Anstalten und Stiftungen gegenüber dem Vorstand oder dem sonst vertretungsberechtigten Organ und fordert zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf. In den Fällen des Satzes 1 Nr.2 und 3 unterrichtet der Berliner Beauftragte für Datenschutz und Informationsfreiheit gleichzeitig auch das für die Aufsicht zuständige Mitglied des Senats.

(2) Der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(3) Mit der Beanstandung kann der Berliner Beauftragte für Datenschutz und Informationsfreiheit Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(4) Die nach Absatz 1 Satz 1 abzugebende Stellungnahme soll auch eine Darstellung der Maßnahmen enthalten, die auf Grund der Beanstandung des Berliner Beauftragten für Datenschutz und Informationsfreiheit getroffen worden sind. Die in Absatz 1 Satz 1 Nr.2 und 3 genannten Stellen leiten dem für die Aufsicht zuständigen Mitglied des Senats eine Abschrift ihrer Stellungnahme an den Berliner Beauftragten für Datenschutz und Informationsfreiheit zu.

§ 27
Anrufung

Jedermann kann sich an den Berliner Beauftragten für Datenschutz und Informationsfreiheit wenden, wenn er der Ansicht ist, dass bei der Verarbeitung personenbezogener Daten durch Behörden oder sonstige öffentliche Stellen gegen die Vorschriften dieses Gesetzes oder gegen andere Datenschutzvorschriften verstoßen worden ist oder ein solcher Verstoß bevorsteht. Dies gilt auch für Dienstkräfte der Behörden und sonstigen öffentlichen Stellen, ohne dass der Dienstweg einzuhalten ist.

§ 28
Unterstützung

(1) Die Behörden und sonstigen öffentlichen Stellen sind verpflichtet, den Berliner Beauftragten für Datenschutz und Informationsfreiheit und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ihnen sind dabei insbesondere

1. Auskunft zu ihren Fragen sowie Einsicht in alle Unterlagen und Akten zu gewähren, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, namentlich in die gespeicherten Daten und in die Datenverarbeitungsprogramme,

2. die in Nummer 1 genannten Unterlagen und Akten herauszugeben und Kopien von Unterlagen, von automatisierten Dateien, von deren Verfahren und von organisatorischen Regelungen zur Mitnahme zur Verfügung zu stellen,

3. jederzeit Zutritt in alle Diensträume und Zugriff auf elektronische Einrichtungen zu gewähren. Satz 2 gilt für die in § 19a Abs. 1 Satz 7 genannten Aufgaben nicht, soweit das jeweils zuständige Mitglied des Senats im Einzelfall feststellt, dass die Einsicht in die Unterlagen und Akten die Sicherheit des Bundes oder eines Landes gefährdet. Auf Antrag des Berliner Beauftragten für Datenschutz und Informationsfreiheit hat die Senatsverwaltung dies im zuständigen Ausschuss des Abgeordnetenhauses in geheimer Sitzung zu begründen. Die Entscheidung des Ausschusses kann veröffentlicht werden.

(2) Berufs- und Amtsgeheimnisse entbinden nicht von der Unterstützungspflicht.

§ 29
Berichte und Gutachten

(1) Auf Anforderung des Abgeordnetenhauses oder des Senats hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit Gutachten zu erstellen und Berichte zu erstatten.

(2) Er hat dem Abgeordnetenhaus und dem Senat jährlich einen Bericht über das Ergebnis seiner Tätigkeit vorzulegen. Der Senat legt dem Abgeordnetenhaus regelmäßig innerhalb von drei Monaten nach Vorlage des Berichts eine Stellungnahme zu dem Bericht vor.

(3) Auf Ersuchen des Abgeordnetenhauses, des Petitionsausschusses des Abgeordnetenhauses oder des Senats hat der Berliner Beauftragte für Datenschutz und Informationsfreiheit ferner Hinweisen auf Angelegenheiten und Vorgänge, die seinen Aufgabenkreis unmittelbar betreffen, nachzugehen. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit kann sich jederzeit an das Abgeordnetenhaus wenden.

Fünfter Abschnitt
Besonderer Datenschutz

§ 30
Datenverarbeitung für wissenschaftliche Zwecke

(1) Zum Zwecke wissenschaftlicher Forschung dürfen datenverarbeitende Stellen personenbezogene Daten ohne Einwilligung des Betroffenen nur für bestimmte Forschungsarbeiten übermitteln,

1. soweit dessen schutzwürdige Belange wegen der Art der Daten, wegen ihrer Offenkundigkeit oder wegen der Art der Verwendung nicht beeinträchtigt werden, oder

2. wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen erheblich überwiegt und der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Die Übermittlung bedarf der vorherigen Zustimmung der obersten Landesbehörde oder einer von dieser bestimmten Stelle; dies gilt nicht für die öffentlichen Stellen nach § 2 Abs. 3. Die Zustimmung muss den Empfänger, die Art der zu übermittelnden personenbezogenen Daten, den Kreis der Betroffenen und das Forschungsvorhaben bezeichnen und ist dem Berliner Beauftragten für Datenschutz und Informationsfreiheit mitzuteilen.

(2) Sobald der Forschungszweck dies erlaubt, sind die Merkmale, mit deren Hilfe ein Personenbezug hergestellt werden kann, gesondert zu speichern, die Merkmale sind zu löschen, sobald der Forschungszweck erreicht ist.

(3) Eine Verarbeitung der nach Absatz 1 übermittelten Daten zu anderen als Forschungszwecken ist unzulässig. Die nach Absatz 1 Satz 2 übermittelten Daten dürfen nur mit Einwilligung des Betroffenen weiterübermittelt werden.

(4) Soweit die Vorschriften dieses Gesetzes auf den Empfänger keine Anwendung finden, dürfen personenbezogene Daten nur übermittelt werden, wenn sich der Empfänger verpflichtet, die Vorschriften der Absätze 2 und 3 einzuhalten, und sich der Kontrolle des Berliner Beauftragten für Datenschutz und Informationsfreiheit unterwirft.

(5) Die wissenschaftliche Forschung betreibenden öffentlichen Stellen dürfen personenbezogene Daten nur veröffentlichen, wenn

a) der Betroffene eingewilligt hat oder

b) dieses für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

(6) Unter den Voraussetzungen des Absatzes 1 darf die datenverarbeitende Stelle personenbezogene Daten ohne Einwilligung des Betroffenen selbst zum Zwecke wissenschaftlicher Forschung verarbeiten.

§ 31
Datenverarbeitung durch den Sender Freies Berlin

(1) Soweit der Sender Freies Berlin personenbezogene Daten ausschließlich zu eigenen journalistisch-redaktionellen oder literarischen Zwecken verarbeitet, gelten anstelle dieses Gesetzes § 22a des Berliner Pressegesetzes vom 15. Juni 1965 (GVBl. S. 744), das zuletzt durch Artikel VI des Gesetzes vom 30. Juli 2001 (GVBl. S. 305) geändert worden ist, und § 41 Abs. 2 und 3 des Bundesdatenschutzgesetzes entsprechend.

(2) Der Sender Freies Berlin bestellt einen Beauftragten für den Datenschutz, der die Vorschriften über den Datenschutz im journalistisch-redaktionellen Bereich frei von Weisungen überwacht. An ihn kann sich jedermann wenden, wenn er annimmt, bei der Verarbeitung personenbezogener Daten zu journalistisch-redaktionellen oder literarischen Zwecken in seinen Rechten verletzt worden zu sein. Beanstandungen richtet der Beauftragte für den Datenschutz an den Intendanten und unterrichtet gleichzeitig den Rundfunkrat. Die Dienstaufsicht obliegt dem Verwaltungsrat.

§ 31a
Fernmess- und Fernwirkdienste

(1) Öffentliche Stellen dürfen ferngesteuerte Messungen oder Beobachtungen (Fernmessdienste) in Wohnungen oder Geschäftsräumen nur vornehmen oder mittels einer Übertragungseinrichtung in Wohnungen oder Geschäftsräumen andere Wirkungen nur auslösen (Fernwirkdienste), wenn der Betroffene zuvor über den Verwendungszweck sowie über Art, Umfang und Zeitraum des Einsatzes des Dienstes unterrichtet worden ist und nach der Unterrichtung schriftlich eingewilligt hat. Der Betroffene kann seine Einwilligung jederzeit widerrufen. Das Abschalten eines Dienstes gilt im Zweifel als Widerruf der Einwilligung.

(2) Die Einrichtung von Fernmess- und Fernwirkdiensten ist nur zulässig, wenn der Betroffene erkennen kann, wann ein Dienst in Anspruch genommen wird und welcher Art dieser Dienst ist, und wenn der Teilnehmer den Dienst jederzeit abschalten kann, soweit dies mit dem Vertragszweck vereinbar ist.

(3) Eine Leistung, der Abschluss oder die Abwicklung eines Vertragsverhältnisses dürfen nicht davon abhängig gemacht werden, dass der Betroffene nach Absatz 1 Satz 1 einwilligt. Verweigert oder widerruft er seine Einwilligung, so dürfen ihm keine Nachteile entstehen, die über die unmittelbaren Folgekosten hinausgehen.

(4) Soweit im Rahmen von Fernmess- und Fernwirkdiensten personenbezogene Daten erhoben werden, dürfen diese nur zu den vereinbarten Zwecken verarbeitet werden. Sie sind zu löschen, wenn sie zur Erfüllung dieser Zwecke nicht mehr erforderlich sind.

§ 31b
Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit der Einsatz der Videoüberwachung zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die datenverarbeitende Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betrof-

fenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(3a) Für Daten, die in öffentlich zugänglichen Räumen des öffentlichen Personennahverkehrs nach Absatz 1 erhoben oder nach Absatz 3 Satz 1 gespeichert werden, gilt anstelle von Absatz 3 Satz 2, dass

1. sie für einen anderen Zweck nur verarbeitet werden dürfen, soweit dies zur Abwehr oder für die Verfolgung von Straftaten erforderlich ist, und

2. für diesen Zweck ihre Übermittlung ausschließlich an den Polizeipräsidenten in Berlin und an die Strafverfolgungsbehörden zulässig ist. Aufzeichnungen, deren Speicherung weder für die Abwehr noch für die Verfolgung von Straftaten erforderlich ist, sind spätestens nach 24 Stunden zu löschen. Dies ist durch ein mit dem Polizeipräsidenten in Berlin abzustimmendes Sicherheitskonzept zu gewährleisten.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung, die Identität der verarbeitenden Stelle sowie über die Zweckbestimmung der Verarbeitung zu benachrichtigen. Der Betroffene ist auch über die Empfänger oder Kategorien von Empfängern von Daten zu unterrichten, soweit er nicht mit der Übermittlung an diese rechnen muss. Sofern eine Übermittlung vorgesehen ist, hat die Unterrichtung spätestens bei der ersten Übermittlung zu erfolgen. Eine Pflicht zur Benachrichtigung besteht nicht, wenn

1. eine Abwägung ergibt, dass das Benachrichtigungsrecht des Betroffenen hinter dem öffentlichen Interesse an der Geheimhaltung aus zwingenden Gründen zurücktreten muss,

2. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,

3. die Unterrichtung des Betroffenen einen unverhältnismäßigen Aufwand erfordert oder

4. die Speicherung oder Übermittlung der personenbezogenen Daten durch Gesetz ausdrücklich vorgesehen ist. Die verantwortliche Stelle legt schriftlich fest, unter welchen Voraussetzungen von einer Benachrichtigung nach Nummer 3 oder 4 abgesehen wird.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 31c
Mobile personenbezogene Speicher- und Verarbeitungsmedien

(1) Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen

1. über ihre Identität und Anschrift,

2. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten,

3. darüber, wie er seine Rechte nach den §§ 16 und 17 ausüben kann, und

4. über die bei Verlust oder Zerstörung des Mediums zu treffenden Maßnahmen unterrichten, soweit der Betroffene nicht bereits Kenntnis erlangt hat.

(2) Die nach Absatz 1 verpflichtete Stelle hat dafür Sorge zu tragen, dass die zur Wahrnehmung des Auskunftsrechts erforderlichen Geräte oder Einrichtungen in angemessenem Umfang zum unentgeltlichen Gebrauch zur Verfügung stehen.

(3) Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, müssen für den Betroffenen eindeutig erkennbar sein.

Sechster Abschnitt
Schlussvorschriften

§ 32
Straftaten

(1) Wer unbefugt personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt oder verändert oder

2. abruft oder sich aus in Behältnissen verschlossenen Dateien verschafft, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so ist die Strafe Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

(3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt ist der Betroffene. Antragsberechtigt ist auch der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Der Berliner Beauftragte für Datenschutz und Informationsfreiheit ist auch gegen den Willen des Betroffenen antragsberechtigt.

§ 33
Aufsichtsbehörde nach dem Bundesdatenschutzgesetz

(1) Aufsichtsbehörde nach dem Bundesdatenschutzgesetz für die Datenverarbeitung nicht öffentlicher Stellen und öffentlich-rechtlicher Wettbewerbsunternehmen ist der Berliner Beauftragte für Datenschutz und Informationsfreiheit. Er untersteht insoweit der Rechtsaufsicht des Senats, die entsprechend der §§ 10 bis 13 des Allgemeinen Zuständigkeitsgesetzes ausgeübt wird.

(2) Die Aufsichtsbehörde erhält von den Gewerbeämtern Durchschriften der An-, Um- bzw. Abmeldungen von Betrieben, die nach dem Kenntnisstand der Gewerbeämter der Meldepflicht des § 4d des Bundesdatenschutzgesetzes unterfallen. Wenn der Aufsichtsbehörde im Rahmen ihrer rechtmäßigen Aufgabenerfüllung Tatsachen bekannt werden, die auf eine gewerberechtliche Unzuverlässigkeit hindeuten, kann sie diese Tatsachen den Gewerbeämtern mitteilen.

(3) Die Aufsichtsbehörde ist befugt, personenbezogene Daten, die ihr im Rahmen von Beschwerden und Anfragen bekannt werden, zu verarbeiten, soweit dies zur Erfüllung ihrer Aufgaben nach dem Bundesdatenschutzgesetz erforderlich ist. Sie darf personenbezogene Daten im Rahmen von Kontrollmaßnahmen im Einzelfall auch ohne Kenntnis der Betroffenen erheben, wenn nur auf diese Weise festgestellt werden kann, ob ein datenschutzrechtlicher Mangel besteht. Die nach den Sätzen 1 und 2 verarbeiteten Daten dürfen nicht zu anderen Zwecken weiterverarbeitet werden.

§ 34
Besondere Regelungen

Abweichend von § 13 ist die Einwilligung des Betroffenen nicht erforderlich bei der Übermittlung personenbezogener Daten aus den Anzeigen Gewerbetreibender nach den §§ 14 und 55c der Gewerbeordnung, soweit die Übermittlung zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist oder soweit der Dritte ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht.

§ 35
Änderung des Gesetzes über das Verfahren der Berliner Verwaltung

(überholt)

§ 36
Inkrafttreten, Außerkrafttreten

(vom Abdruck wird abgesehen)

Anmerkung des Autors:

Im Paragrafen 31 des vorstehenden Gesetzes wird noch die ursprüngliche Senderbezeichnung genannt.

Aufgrund des Staatsvertrages über die Errichtung einer gemeinsamen Rundfunkanstalt der Länder Berlin und Brandenburg vom 25. Juni 2002 wurde der RBB errichtet.

Der RBB nahm am 1. Mai 2003 den Sendebetrieb auf und übernahm die Programme des ehemaligen Sender Freies Berlin (SFB) und des Ostdeutscher Rundfunk Brandenburg (ORB).

Anhang 3: Informationsfreiheitsgesetz

Gesetz zur Regelung des Zugangs zu Informationen des Bundes

Ausfertigungsdatum: 05.09.2005

Vollzitat: "Informationsfreiheitsgesetz vom 5. September 2005 (BGBl. I S. 2722)"

Fußnote Textnachweis ab: 1. 1.2006

§ 1 Grundsatz

(1) Jeder hat nach Maßgabe dieses Gesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen. Für sonstige Bundesorgane und -einrichtungen gilt dieses Gesetz, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Einer Behörde im Sinne dieser Vorschrift steht eine natürliche Person oder juristische Person des Privatrechts gleich, soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient.

(2) Die Behörde kann Auskunft erteilen, Akteneinsicht gewähren oder Informationen in sonstiger Weise zur Verfügung stellen. Begehrt der Antragsteller eine bestimmte Art des Informationszugangs, so darf dieser nur aus wichtigem Grund auf andere Art gewährt werden. Als wichtiger Grund gilt insbesondere ein deutlich höherer Verwaltungsaufwand.

(3) Regelungen in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen gehen mit Ausnahme des § 29 des Verwaltungsverfahrensgesetzes und des § 25 des Zehnten Buches Sozialgesetzbuch vor.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist

1. amtliche Information: jede amtlichen Zwecken dienende Aufzeichnung, unabhängig von der Art ihrer Speicherung. Entwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen, gehören nicht dazu;

2. Dritter: jeder, über den personenbezogene Daten oder sonstige Informationen vorliegen.

§ 3 Schutz von besonderen öffentlichen Belangen

Der Anspruch auf Informationszugang besteht nicht,

1. wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf

a) internationale Beziehungen,

b) militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr,

c) Belange der inneren oder äußeren Sicherheit,

d) Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden,

e) Angelegenheiten der externen Finanzkontrolle,

f) Maßnahmen zum Schutz vor unerlaubtem Außenwirtschaftsverkehr,

g) die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitsrechtlicher oder disziplinarischer Ermittlungen,

2. wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann,

3. wenn und solange

a) die notwendige Vertraulichkeit internationaler Verhandlungen oder

b) die Beratungen von Behörden beeinträchtigt werden,

4. wenn die Information einer durch Rechtsvorschrift oder durch die Allgemeine Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen geregelten Geheimhaltungs- oder Vertraulichkeitspflicht oder einem Berufs- oder besonderen Amtsgeheimnis unterliegt,

5. hinsichtlich vorübergehend beigezogener Information einer anderen öffentlichen Stelle, die nicht Bestandteil der eigenen Vorgänge werden soll,

6. wenn das Bekanntwerden der Information geeignet wäre, fiskalische Interessen des Bundes im Wirtschaftsverkehr oder wirtschaftliche Interessen der Sozialversicherungen zu beeinträchtigen,

7. bei vertraulich erhobener oder übermittelter Information, soweit das Interesse des Dritten an einer vertraulichen Behandlung im Zeitpunkt des Antrags auf Informationszugang noch fortbesteht,

8. gegenüber den Nachrichtendiensten sowie den Behörden und sonstigen öffentlichen Stellen des Bundes, soweit sie Aufgaben im Sinne des § 10 Nr. 3 des Sicherheitsüberprüfungsgesetzes wahr-nehmen.

§ 4 Schutz des behördlichen Entscheidungsprozesses

(1) Der Antrag auf Informationszugang soll abgelehnt werden für Entwürfe zu Entscheidungen sowie Arbeiten und Beschlüsse zu ihrer unmittelbaren Vorbereitung, soweit und solange durch die vorzeitige Bekanntgabe der Informationen der Erfolg der Entscheidung oder bevorstehender behördlicher Maß-

nahmen vereitelt würde. Nicht der unmittelbaren Entscheidungsvorbereitung nach Satz 1 dienen regelmäßig Ergebnisse der Beweiserhebung und Gutachten oder Stellungnahmen Dritter.

(2) Der Antragsteller soll über den Abschluss des jeweiligen Verfahrens informiert werden.

§ 5 Schutz personenbezogener Daten

(1) Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 des Bundesdatenschutzgesetzes dürfen nur übermittelt werden, wenn der Dritte ausdrücklich eingewilligt hat.

(2) Das Informationsinteresse des Antragstellers überwiegt nicht bei Informationen aus Unterlagen, soweit sie mit dem Dienst- oder Amtsverhältnis oder einem Mandat des Dritten in Zusammenhang stehen und bei Informationen, die einem Berufs- oder Amtsgeheimnis unterliegen.

(3) Das Informationsinteresse des Antragstellers überwiegt das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs in der Regel dann, wenn sich die Angabe auf Name, Titel, akademischen Grad, Berufs- und Funktions-bezeichnung, Büroanschrift und –telekommunikationsnummer beschränkt und der Dritte als Gutachter, Sachverständiger oder in vergleichbarer Weise eine Stellungnahme in einem Verfahren abgegeben hat.

(4) Name, Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer von Bearbeitern sind vom Informationszugang nicht ausgeschlossen, soweit sie Ausdruck und Folge der amtlichen Tätigkeit sind und kein Ausnahmetatbestand erfüllt ist.

§ 6 Schutz des geistigen Eigentums und von Betriebs- oder Geschäftsgeheimnissen

Der Anspruch auf Informationszugang besteht nicht, soweit der Schutz geistigen Eigentums entgegensteht. Zugang zu Betriebs- oder Geschäftsgeheimnissen darf nur gewährt werden, soweit der Betroffene eingewilligt hat.

§ 7 Antrag und Verfahren

(1) Über den Antrag auf Informationszugang entscheidet die Behörde, die zur Verfügung über die begehrten Informationen berechtigt ist. Im Fall des § 1 Abs. 1 Satz 3 ist der Antrag an die Behörde zu richten, die sich der natürlichen oder juristischen Person des Privatrechts zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient. Betrifft der Antrag Daten Dritter im Sinne von § 5 Abs. 1 und 2 oder § 6, muss er begründet werden. Bei gleichförmigen Anträgen von mehr als 50 Personen gelten die §§ 17 bis 19 des Verwaltungsverfahrensgesetzes entsprechend.

(2) Besteht ein Anspruch auf Informationszugang zum Teil, ist dem Antrag in dem Umfang stattzugeben, in dem der Informationszugang ohne Preisgabe der geheimhaltungsbedürftigen Informationen oder ohne unverhältnismäßigen Verwaltungsaufwand möglich ist. Entsprechendes gilt, wenn sich der Antragsteller in den Fällen, in denen Belange Dritter berührt sind, mit einer Unkenntlichmachung der diesbezüglichen Informationen einverstanden erklärt.

(3) Auskünfte können mündlich, schriftlich oder elektronisch erteilt werden. Die Behörde ist nicht verpflichtet, die inhaltliche Richtigkeit der Information zu prüfen.

(4) Im Fall der Einsichtnahme in amtliche Informationen kann sich der Antragsteller Notizen machen oder Ablichtungen und Ausdrucke fertigen lassen. § 6 Satz 1 bleibt unberührt.

(5) Die Information ist dem Antragsteller unter Berücksichtigung seiner Belange unverzüglich zugänglich zu machen. Der Informationszugang soll innerhalb eines Monats erfolgen. § 8 bleibt unberührt.

§ 8 Verfahren bei Beteiligung Dritter

(1) Die Behörde gibt einem Dritten, dessen Belange durch den Antrag auf Informationszugang berührt sind, schriftlich Gelegenheit zur Stellungnahme innerhalb eines Monats, sofern Anhaltspunkte dafür vorliegen, dass er ein schutzwürdiges Interesse am Ausschluss des Informationszugangs haben kann.

(2) Die Entscheidung nach § 7 Abs. 1 Satz 1 ergeht schriftlich und ist auch dem Dritten bekannt zu geben. Der Informationszugang darf erst erfolgen, wenn die Entscheidung dem Dritten gegenüber bestandskräftig ist oder die sofortige Vollziehung angeordnet worden ist und seit der Bekanntgabe der Anordnung an den Dritten zwei Wochen verstrichen sind. § 9 Abs. 4 gilt entsprechend.

§ 9 Ablehnung des Antrags; Rechtsweg

(1) Die Bekanntgabe einer Entscheidung, mit der der Antrag ganz oder teilweise abgelehnt wird, hat innerhalb der Frist nach § 7 Abs. 5 Satz 2 zu erfolgen.

(2) Soweit die Behörde den Antrag ganz oder teilweise ablehnt, hat sie mitzuteilen, ob und wann der Informationszugang ganz oder teilweise zu einem späteren Zeitpunkt voraussichtlich möglich ist.

(3) Der Antrag kann abgelehnt werden, wenn der Antragsteller bereits über die begehrten Informationen verfügt oder sich diese in zumutbarer Weise aus allgemein zugänglichen Quellen beschaffen kann.

(4) Gegen die ablehnende Entscheidung sind Widerspruch und Verpflichtungsklage zulässig. Ein Widerspruchsverfahren nach den Vorschriften des 8. Abschnitts der Verwaltungsgerichtsordnung ist auch dann

durchzuführen, wenn die Entscheidung von einer obersten Bundesbehörde getroffen wurde.

§ 10 Gebühren und Auslagen

(1) Für Amtshandlungen nach diesem Gesetz werden Gebühren und Auslagen erhoben. Dies gilt nicht für die Erteilung einfacher Auskünfte.

(2) Die Gebühren sind auch unter Berücksichtigung des Verwaltungsaufwandes so zu bemessen, dass der Informationszugang nach § 1 wirksam in Anspruch genommen werden kann.

(3) Das Bundesministerium des Innern wird ermächtigt, für Amtshandlungen nach diesem Gesetz die Gebührentatbestände und Gebührensätze durch Rechtsverordnung ohne Zustimmung des Bundesrates zu bestimmen. § 15 Abs. 2 des Verwaltungskostengesetzes findet keine Anwendung.

§ 11 Veröffentlichungspflichten

(1) Die Behörden sollen Verzeichnisse führen, aus denen sich die vorhandenen Informations-sammlungen und -zwecke erkennen lassen.

(2) Organisations- und Aktenpläne ohne Angabe personenbezogener Daten sind nach Maßgabe dieses Gesetzes allgemein zugänglich zu machen.

(3) Die Behörden sollen die in den Absätzen 1 und 2 genannten Pläne und Verzeichnisse sowie weitere geeignete Informationen in elektronischer Form allgemein zugänglich machen.

§ 12 Bundesbeauftragter für die Informationsfreiheit

(1) Jeder kann den Bundesbeauftragten für die Informationsfreiheit anrufen, wenn er sein Recht auf Informationszugang nach diesem Gesetz als verletzt ansieht.

(2) Die Aufgabe des Bundesbeauftragten für die Informationsfreiheit wird von dem Bundesbeauftragten für den Datenschutz wahrgenommen.

(3) Die Bestimmungen des Bundesdatenschutz-gesetzes über die Kontrollaufgaben des Bundesbeauftragten für den Datenschutz (§ 24 Abs. 1 und 3 bis 5), über Beanstandungen (§ 25 Abs. 1 Satz 1 Nr. 1 und 4, Satz 2 und Abs. 2 und 3) sowie über weitere Aufgaben gemäß § 26 Abs. 1 bis 3 gelten entsprechend.

§ 13

-

§ 14 Bericht und Evaluierung

Die Bundesregierung unterrichtet den Deutschen Bundestag zwei Jahre vor Außerkrafttreten über die Anwendung dieses Gesetzes. Der Deutsche Bundestag wird das Gesetz ein Jahr vor Außerkrafttreten auf wissenschaftlicher Grundlage evaluieren.

§ 15 Inkrafttreten

Dieses Gesetz tritt am 1. Januar 2006 in Kraft.

Anhang 4: Die bekanntesten Betriebssysteme

DOS auf x86-Basis (DOS für IBM-PC-Kompatible)
- QDOS, CP/M-Kopie für 8086-Prozessoren, von Seattle Computer Products
- MS-DOS, von der Firma Microsoft aufgekauftes und weiter entwickeltes QDOS
- PC-DOS, die MS-DOS-Variante von IBM
- DR-DOS, wohl erfolgreichster MS-DOS-Konkurrent von Digital Research

Netzwerkserversysteme für DOS-Programme
- Novell NetWare, Serverbetriebssystem von Novell. Wird aus (Novell) DOS geladen

Win16-basiert (auf MS-DOS laufend)
- Windows 1.0 erste MS-Windows-Version 1985
- Windows 3.0 erste „moderne“ Microsoft-Windows-Version
- Windows 3.1/3.11 erste kommerziell erfolgreiche Microsoft-Windows-Versionen
- Windows for Workgroups 3.x wie Windows 3.x, mit Netzwerk-Erweiterungen

Win32-basiert (auf MS-DOS laufend)
- Windows 95 a, b, c (c wird auch Windows 96 genannt)
- Windows 98, Windows 98 SE
- Windows ME

auf Basis von Windows NT
- Windows NT 3.1, Microsoft Windows NT 3.5 (mit älterer Windows-3.1-Optik)
- Windows NT 4.0 (mit neuerer Windows-95-Optik, x86, auch: PPC/Alpha/MIPS)
- Windows 2000 (32/64-bit nur Itanium)
- Windows XP (32/64-bit)
- Windows Vista (32/64-bit)

Unix
- UNIX V1-V7 (1969–1979), AT&T
- System V kommerziell vertriebener Quellcode von UNIX, ab 1983

AT&T-System V-Linie
- AIX UNIX Version der Firma IBM
- AMIX UNIX Version für Amiga-Rechner
- Sinix UNIX Version der Firma Siemens
- Solaris UNIX der Firma Sun Microsystems

BSD – Berkeley-Linie (historisch)]
- SunOS 1.0 bis 4.1.4 (Sun Operating System) UNIX der Firma Sun
- Ultrix UNIX der Firma DEC für VAX-Computer (später auch MIPS-Workstations)
- Xenix UNIX Version, ursprünglich der Firma Microsoft

BSD – Berkeley-Linie (modern)
- Darwin Bestandteil von Mac OS X

weitere Unix-Derivate

- NetWare, Serverbetriebssystem von Novell auf Unix-Basis

Desktoprechnersysteme (für Intel x86 Prozessoren)
- OS/2 PC-Betriebssystem von IBM. Aktueller Nachfolger eComStation
- Visopsys minimales Betriebssystem

Macintosh-Systeme von Apple(eigentlich BSD-Derivate)
- System Macintosh Betriebssystem bis System 7.5
- Mac OS Mac OS 7.5.1 bis Mac OS 9.2.2
- Mac OS X

Desktoprechnersysteme (andere Prozessoren)
- AmigaOS AmigaOS 4 / OS4 für AmigaOne von Hyperion Entertainment und Amiga mit Cyberstorm-Erweiterung

Desktoprechnersysteme (portabel)
- GNU/Linux

PDA- und Smartphone-Betriebssysteme
- OS X Betriebssystem für iPhone und iPod Touch
- EPOC Betriebssystem für Psion-Handhelds
- GEOS-SC Betriebssystem für Smartphones
- GNU/Linux (siehe dazu auch Linux-Einsatzbereiche)
- Newton OS, Betriebssystem für den Newton (PDA) von Apple
- PalmDOS, verwendet auf Bildschirm-Schreibmaschinen von Olivetti
- Palm OS Betriebssystem für PALM Handhelds
- Symbian OS Das Betriebssystem, welches auf Nokia und Sony Ericsson Smartphones, der Psion-Plattform sowie einigen Smartphones von Motorola, Sendo und Siemens läuft
- Windows CE/PocketPC

Großrechnersysteme
- BS3000 IBM-kompatibles Betriebssystem der Firma Siemens AG (historisch)
- Fortran Monitor System (FMS)

Frühe Betriebssysteme (historisch)
- GEOS Diverse Plattformen, ursprünglich Commodore C64.

Anhang 5: Die Betriebssysteme der Firma Microsoft

16-Bit-Versionen von Microsoft Windows (Erscheinungsdatum in Klammern):
- Windows 1.0 (20. November 1985)
- Windows 2.0 (November 1987)
- Windows 3.0 (22. Mai 1990)
- Windows 3.1 (1. März 1992)
- Windows 3.11 (Dezember 1993) (nur Übernahme von Treibern aus WfW 3.11)
- Windows 3.2 (1994; nur in China)
- Windows for Workgroups 3.1 (Oktober 1992, Codename „Sparta“)
- Windows for Workgroups 3.11 (1993)

Windows-9x-basierte Versionen (Erscheinungsdatum in Klammern)
- Windows 95
- Windows 95 (15. August 1995, Codename „Chicago“)
- Windows 95a (Februar 1996, Codename „Nashville“)
- Windows 95b (Juli 1996)
- Windows 95b (März 1996)
- Windows 95c (November 1997)
- Windows 98
- Windows 98 (30. Juni 1998, Codename „Memphis“)
- Windows 98 SE (Mai 1999), SE steht für Second Edition (Zweite Ausgabe)
- Windows Me (August/September 2000, Codename „Georgia“),
- Me (offiziell kleines „e“) steht für Millennium Edition

NT-basierte Versionen (Erscheinungsdatum in Klammern)
- Microsoft Windows NT:
- Microsoft Windows NT 3.1 (Juli 1993)
- Microsoft Windows NT Workstation 3.1 (1993)
- Microsoft Windows NT Advanced Server 3.1 (1993)
- Microsoft Windows NT 3.5 (September 1994, Codename „Daytona“)
- Microsoft Windows NT Workstation 3.5 (1994)
- Microsoft Windows NT Server 3.5 (1994)
- Microsoft Windows NT 3.51 (Mai 1995)
- Microsoft Windows NT Workstation 3.51 (1995)
- Microsoft Windows NT Server 3.51 (1995)
- Microsoft Windows NT 4.0 (29. August 1996, Codename „Shell Update Release“)
- Microsoft Windows NT Workstation 4.0 (1996)
- Microsoft Windows NT Server 4.0 (1996)
- Microsoft Windows NT Server 4.0 Enterprise Edition (1997)
- Microsoft Windows NT Server 4.0 Terminal Server Edition (1998)
- Microsoft Windows 2000 (NT Version 5.0, Februar 2000)
- Microsoft Windows 2000 Professional
- Microsoft Windows 2000 Server
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 Datacenter Server
- Microsoft Windows XP (NT Version 5.1, 25. Oktober 2001, Codename „Whistler“)

- Microsoft Windows XP Starter Edition (2004)
- Microsoft Windows XP Home Edition
- Microsoft Windows XP Home Edition N
- (Windows-Version ohne vorinstallierten Windows Media Player, 2005)
- Microsoft Windows XP Professional
- Microsoft Windows XP Professional x64 Edition (2005)
- Microsoft Windows XP Professional N
- (Windows-Version ohne vorinstallierten Windows Media Player, 2005)
- Windows XP Media Center Edition
- Windows XP Media Center Edition 2002, Codename „eHome“
- (Nur in den USA und China)
- Windows XP Media Center Edition 2003, Codename „Freestyle“
- Windows XP Media Center Edition 2004, Codename „Harmony“
- (Erste Version in Europa)
- Windows XP Media Center Edition 2005, Codename „Symphony“
- Windows XP Tablet PC Edition (2002)
- Windows XP Tablet PC Edition 2004 (2004)
- Microsoft Windows PE (Microsoft Windows Preinstallation Environment/XP-Kernel)
- Microsoft Windows Fundamentals for Legacy PCs
- (WinFLP, Codenamen „Mönch“, „Eiger“, Thin-Client-Versionen von XP, 2006)
- Microsoft Windows XP Embedded (2001)
- Microsoft Windows Embedded for Point of Service (2004)
- Microsoft Windows Server 2003 (NT Version 5.2, 2003)
- Microsoft Windows Server 2003 Standard Edition
- Microsoft Windows Server 2003 x64 Standard Edition (2005)
- Microsoft Windows Server 2003 Enterprise Edition
- Microsoft Windows Server 2003 x64 Enterprise Edition (2005)
- Microsoft Windows Server 2003 Datacenter Edition
- Microsoft Windows Server 2003 x64 Datacenter Edition (2005)
- Microsoft Windows Server 2003 Web Edition
- Microsoft Windows Vista
- (NT Version 6.0, für Privatbenutzer 30. Januar 2007; für Firmen bzw. Unternehmen 30. November 2006, Codename „Longhorn“)
- Microsoft Windows Vista Starter (nicht in Europa)
- Microsoft Windows Vista Home Basic
- Microsoft Windows Vista Home Basic N
- Microsoft Windows Vista Home Basic K (nur Korea ohne Mediaplayer und Instant Messenger)
- Microsoft Windows Vista Home Premium
- Microsoft Windows Vista Business
- Microsoft Windows Vista Business N
- Microsoft Windows Vista Business K (nur Korea ohne Mediaplayer und Instant Messenger)
- Microsoft Windows Vista Enterprise
- Microsoft Windows Vista Ultimate
- Microsoft Windows Home Server
- Microsoft Windows Server 2008, ehemals Longhorn Server
- Microsoft Windows 7, ehemals „Vienna“, ehemals „Blackcomb“

Anhang: 6 Einen Serienbrief erstellen

Um einen Serienbrief zu erstellen, benötigt man im Mustervorgang neben den Anschriften auch einen Brieftext, den jeder Empfänger erhalten soll.

Zur Zielerreichung bieten sich mehrere Varianten an, die im Folgenden anhand der Standardtextverarbeitung Microsoft Word 2003 erklärt werden.

Nachdem Word gestartet wurde, werden in einem ersten Schritt lediglich die Daten erfasst. Dabei können die Daten in Form einer Tabelle oder durch Feldtrennzeichen erfasst werden. Als Feldtrennzeichen wird üblicher Weise das Semikolon (;) verwendet – andere Feldtrennzeichen sind denkbar.

In beiden Fällen werden in der ersten Zeile die Feldnamen angegeben:

entweder

Name;Vorname;Straße;PLZ;Ort,Anrede

oder

Name	*Vorname*	*Straße*	*PLZ*	*Ort*	*Anrede*

In den folgenden Zeilen werden anschließend die Daten der Empfänger erfasst.

entweder

Müller;Michael;Musterweg 1;12345;Berlin;Herrn
Schmidt;Sabine;Poststraße 2;23456;Hamburg;Frau
Lehmann;Peter;Dorfgasse 3;01234;Dresden;Herrn
Schulz;Lisa;Bergallee 4;19045;Güstrow;Frau

oder

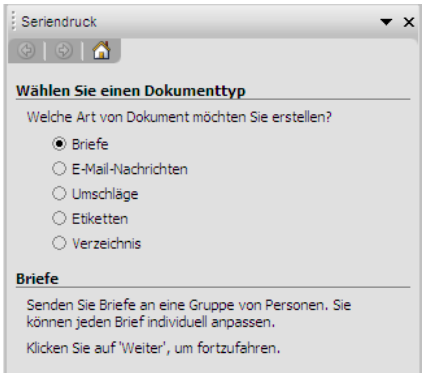
Müller	*Michael*	*Musterweg 1*	*12345*	*Berlin*	*Herrn*
Schmidt	*Sabine*	*Poststraße 2*	*23456*	*Hamburg*	*Frau*
Lehmann	*Peter*	*Dorfgasse 3*	*01234*	*Dresden*	*Herrn*
Schulz	*Lisa*	*Bergallee 4*	*19045*	*Güstrow*	*Frau*

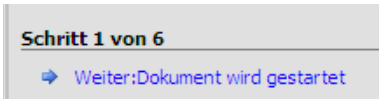
Die somit erstellte Steuersatzdatei wird nun gespeichert. Eine Steuersatzdatei kann auch unter der Verwendung von Microsoft Excel oder Microsoft Access erstellt werden. Bitte verwenden Sie einen eindeutigen Dateinamen, den Sie im Folgenden leicht wieder erkennen können, zum Beispiel Steuersatzdatei.doc (bei der Verwendung von Excel lautet die Dateierweiterung .xls, bei Access .mdb).

Schließen Sie die Datei. Der erste Schritt ist somit erledigt.

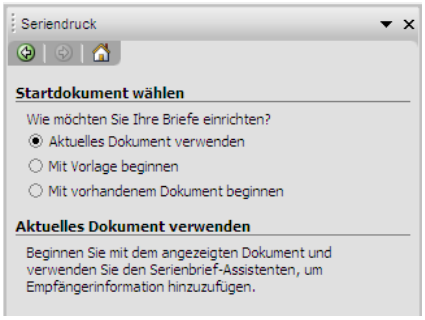
Im nächsten Schritt öffnen Sie eine neue leere Dokumentenseite und erfassen nun den Text, den alle Empfänger erhalten sollen.
Speichern Sie dieses Dokument ebenfalls wieder unter einem Dateinamen ab, den Sie leicht wieder erkennen können, zum Beispiel Textdatei.doc.
Nun starten Sie aus dem Menü Extras die Serienbrieferstellung mit Briefe und Sendungen und anschließend Serienbrieferstellung.
An dieser Stelle kann es bei Vorgängerversionen zu anderen Menüfolgen kommen, die aber keinen Einfluss auf die Serienbrieferstellung haben.
Am rechten Bildschirmrand öffnet sich nun der Seriendruckassistent, der Sie in sechs Schritten zum Ziel führt.

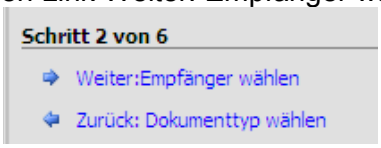
Im Schritt 1 werden Sie gefragt, welche Art von Dokument Sie erstellen möchten. In diesem Fall befassen wir uns ausschließlich mit der Dokumentenart Brief. Sofern Sie sich nicht sicher sind welches Optionsfeld richtig ist, können Sie jeweils unter den Wahlmöglichkeiten nach dem Klick auf die Optionsschaltfläche eine kurze Beschreibung lesen. Um zum Schritt 2 zu gelangen, klicken Sie weiter unten auf den Link Weiter: Dokument wird gestartet.



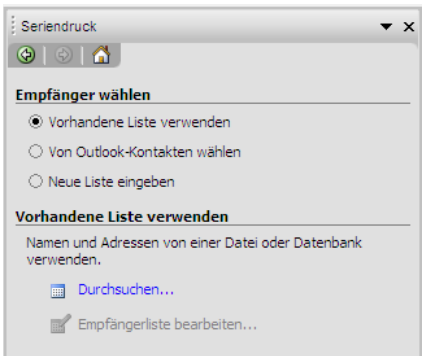


An dieser Stelle muss das Startdokument ausgewählt werden. Da wir in diesem Beispiel bereits einen Brieftext erfasst und geöffnet haben, wählen Sie hier die erste Optionsschaltfläche aus. Sofern Sie den Brieftext geschlossen haben, wählen Sie die dritte Optionsschaltfläche aus; Sie werden dann mit dem Dialog Datei öffnen aufgefordert, den Pfad zur vorhandenen Textdatei auszuwählen. Um zum Schritt 3 zu gelangen, klicken Sie auf den Link Weiter: Empfänger wählen.


Seriendruck
Startdokument wählen
Wie möchten Sie Ihre Briefe einrichten?
Aktuelles Dokument verwenden
Mit Vorlage beginnen
Mit vorhandenem Dokument beginnen
Aktuelles Dokument verwenden
Beginnen Sie mit dem angezeigten Dokument und verwenden Sie den Serienbrief-Assistenten, um Empfängerinformation hinzuzufügen.

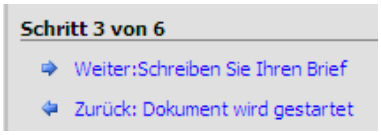


In diesem Beispiel haben wir bereits eine Steuersatzdatei erstellt und abgespeichert. An dieser Stelle muss nun angegeben werden, unter welchem Pfad die Steuersatzdatei abgelegt wurde. Wählen Sie hierzu das erste Optionsfeld aus und klicken anschließend auf den Link Durchsuchen...

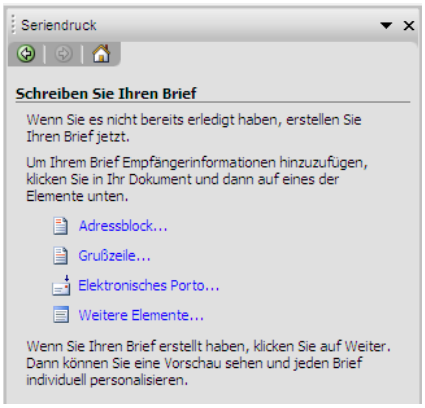


Sie werden dann mit dem Dialog Datei öffnen aufgefordert, den Pfad zur vorhandenen Steuersatzdatei auszuwählen. Nach der Auswahl erscheint der Pfad an der Stelle, wo zuvor der Link Durchsuchen... angezeigt wurde. Auch diesen Schritt haben Sie nun erfolgreich abgeschlossen, sodass Sie zum Schritt 4 wechseln können. Klicken Sie hierzu auf den Link Weiter:

Schreiben Sie Ihren Brief.



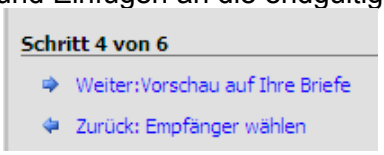
Der Brieftext erscheint nun auf der linken Fensterseite. Es ist nun erforderlich, dass an den Stellen, an denen variable Daten erscheinen sollen, Seriendruckfelder eingefügt werden. Mit dem Wechsel zum Schritt 4 wurde gleichzeitig eine neue Symbolleiste am oberen Bildschirmrand eingefügt. Die meisten Symbole werden bereits farbig dargestellt.


Seriendruck
Schreiben Sie Ihren Brief
Wenn Sie es nicht bereits erledigt haben, erstellen Sie Ihren Brief jetzt.
Um Ihrem Brief Empfängerinformationen hinzuzufügen, klicken Sie in Ihr Dokument und dann auf eines der Elemente unten.
Adressblock...
Grußzeile...
Elektronisches Porto...
Weitere Elemente...
Wenn Sie Ihren Brief erstellt haben, klicken Sie auf Weiter. Dann können Sie eine Vorschau sehen und jeden Brief individuell personalisieren.

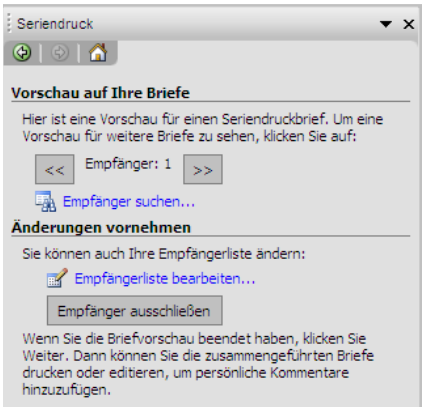
Setzen Sie den Cursor zunächst an die Stelle, an der das Seriendruckfeld eingefügt werden soll. Wählen Sie dann aus der Symbolleiste die Schaltfläche Seriendruckfelder einfügen aus.

Es öffnet sich ein Dialogfeld, in dem alle zur Verfügung stehenden Seriendruckfelder aufgelistet sind. Dabei entsprechen die aufgeführten Feldnamen genau denen, der in der ersten Zeile Ihrer Steuersatzdatei erfassten Namen.

Wählen Sie das Feld mit einem Doppelklick aus – es wird automatisch an der Cursorposition eingefügt. Es ist auch möglich, an dieser Stelle alle benötigten Felder hintereinander in das Dokument zu übernehmen und anschließend mit Hilfe der Funktionen Kopieren/Ausschneiden und Einfügen an die endgültigen Stellen zu positionieren.

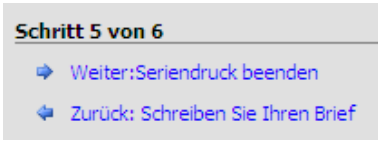


An dieser Stelle können Sie prüfen, ob die Seriendruckfelder richtig positioniert wurden. Mit den Schaltflächen links und rechts neben Empfänger, schalten Sie zwischen den verschiedenen Datensätzen der Steuersatzdatei hin und her. Es ist somit eine Vorschau auf das zu erwartende Ergebnis der Seriendruckerstellung. Überarbeitungen können jederzeit im linken Fensterbereich vorgenommen werden.

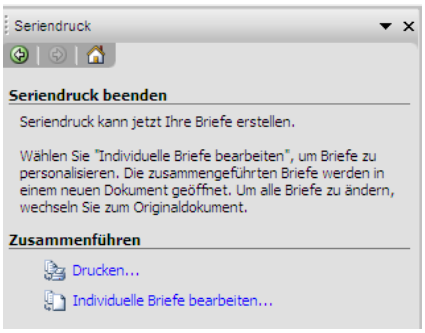

Seriendruck
Vorschau auf Ihre Briefe
Hier ist eine Vorschau für einen Seriendruckbrief. Um eine Vorschau für weitere Briefe zu sehen, klicken Sie auf:
<<
Empfänger: 1
>>
Empfänger suchen...
Änderungen vornehmen
Sie können auch Ihre Empfängerliste ändern:
Empfängerliste bearbeiten...
Empfänger ausschließen
Wenn Sie die Briefvorschau beendet haben, klicken Sie Weiter. Dann können Sie die zusammengeführten Briefe drucken oder editieren, um persönliche Kommentare hinzuzufügen.

Wenn alle Seriendruckfelder eingefügt wurden, schließen Sie diesen Schritt ab und wechseln mit einem Klick auf Weiter: Vorschau auf Ihre Briefe zum Schritt 5.

Sofern Sie alle Anpassungen vorgenommen haben, gehen Sie mit einem Klick auf Weiter: Seriendruck beenden zum letzten Schritt.

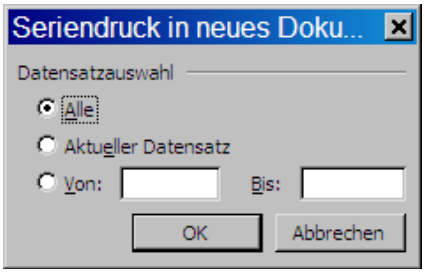


Zum Abschluss müssen Sie auswählen, ob die Serienbriefe direkt an den Drucker gesendet werden sollen, oder ob Sie eventuell individuelle Ergänzungen in einzelnen Briefen vornehmen möchten. Individuelle Ergänzungen sind beispielsweise denkbar, wenn Sie bestimmten Empfängern persönliche Zeilen anfügen möchten.


Seriendruck
Seriendruck beenden
Seriendruck kann jetzt Ihre Briefe erstellen.
Wählen Sie "Individuelle Briefe bearbeiten", um Briefe zu personalisieren. Die zusammengeführten Briefe werden in einem neuen Dokument geöffnet. Um alle Briefe zu ändern, wechseln Sie zum Originaldokument.
Zusammenführen
Drucken...
Individuelle Briefe bearbeiten...

In beiden Fällen erscheint nach dem Klick auf den Link ein Dialogfeld, in dem Sie angeben können, welche Datensätze in die Seriendruckerstellung mit einbezogen werden sollen. In der Regel werden an dieser Stelle ALLE Datensätze ausgewählt.

Je nach Auswahl finden Sie die fertigen Serienbriefe im Ausgabefach des Druckers bzw. als neue Datei (Seriendruck1) am Bildschirm. Die am Bildschirm angezeigten Serienbriefe können Sie in einer eigenen Datei abspeichern.



Anhang 7: Netzwerktopologien

Um die Arbeitsweise von Netzwerken zu verstehen, müssen einige Grundbegriffe der verschiedenen Topologien (physikalische Strukturen) bekannt sein.

Stern-Topologie

Bei Netzen in Stern-Topologie sind an einen zentralen Teilnehmer alle anderen Teilnehmer mit einer Zweipunktverbindung angeschlossen. Der zentrale Teilnehmer muss nicht notwendigerweise über eine besondere Steuerungsintelligenz verfügen. In Transportnetzen ist das generell nicht der Fall. In Computernetzen kann es eine spezialisierte Einrichtung sein, zum Beispiel ein Hub oder Switch. Auch eine Nebenstellenanlage ist gewöhnlich als Sternnetz aufgebaut: Die Vermittlungsanlage ist der zentrale Knoten, an den die Teilnehmerapparate sternförmig angeschlossen sind.

In jedem Fall bewirkt eine zentrale Komponente in einem Netz eine höhere Ausfallwahrscheinlichkeit für die einzelnen Verbindungen: ein Ausfall des zentralen Teilnehmers bewirkt unweigerlich den Ausfall aller Verbindungsmöglichkeiten zur gleichen Zeit. Eine geläufige Schutzmaßnahme bei Sternnetzen besteht darin, die zentrale Komponente zu doppeln (Redundanz).

Vorteile:

- Der Ausfall eines Endgerätes hat keine Auswirkung auf den Rest des Netzes.
- Dieses Netz bietet hohe Übertragungsraten, wenn der Netzknoten ein Switch ist.
- Leicht erweiterbar
- Leicht verständlich
- Leichte Fehlersuche
- Kombinierte Telefon- / Rechnernetzverkabelung möglich
- Sehr gute Eignung für Multicast-/Broadcastanwendungen
- Kein Routing benötigt

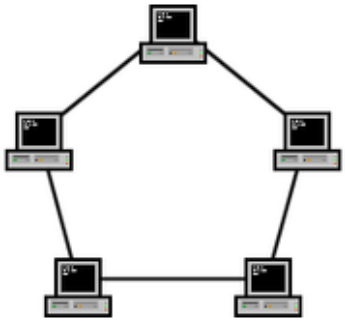
Nachteile:

- Durch Ausfall des Verteilers wird Netzverkehr unmöglich
- Niedrige Übertragungsrate bei vielen Hosts wenn ein Hub benutzt wird ✳ Unterteilung des Netzes mit Switch ist notwendig

Beispiele:

- Telefonnetz
- Fast Ethernet (physisch)
- Token Ring (physisch)

Ring-Topologie



Bei der Vernetzung in Ring-Topologie werden jeweils 2 Teilnehmer über Zweipunktverbindungen miteinander verbunden, so dass ein geschlossener Ring entsteht. Die zu übertragende Information wird von Teilnehmer zu Teilnehmer weitergeleitet, bis sie ihren Bestimmungsort erreicht. Um Überschneidungen zu verhindern, sind bei dieser Art der Vernetzung besondere Adressierungsverfahren nötig. Da jeder Teilnehmer gleichzeitig als Repeater wirken kann (wenn keine Splitter eingesetzt werden), können auf diese Art große Entfernungen überbrückt werden; bei Verwendung von Lichtwellenleitern (LWL) im Kilometerbereich.

Bei einem Ausfall einer der Teilnehmer bricht das gesamte Netz zusammen, es sei denn, die Teilnehmer beherrschen Protection-Umschaltung. In einem Ring mit Protection wird häufig der Arbeitsweg in einer bestimmten Drehrichtung um den Ring geführt (beispielsweise im Uhrzeigersinn), der Ersatzweg in der anderen Drehrichtung (im Beispiel gegen den Uhrzeigersinn).

Eine Sonderform der Ring-Topologie ist die Linien-Topologie, bei der es sich um einen "offenen Ring" handelt, d. h. der erste und der letzte Rechner sind nicht miteinander verbunden. Dieses System ist sehr einfach aufzubauen aber auch sehr anfällig, da der Ausfall eines Rechners die gesamte weitere Datenübertragung unmöglich macht.

Vorteile:

- Deterministische Rechnernetzkommunikation - Vorgänger und Nachfolger sind definiert
- Alle Stationen arbeiten als Verstärker
- Keine Kollisionen
- Alle Rechner haben gleiche Zugriffsmöglichkeiten
- Garantierte Übertragungsbandbreite
- skaliert sehr gut, Grad bleibt bei Erweiterung konstant
- reguläre Topologie, daher leicht programmierbar

Nachteile:

- niedrige Bisektionsweite1 und Konnektivität2, d.h. einerseits, dass der Ausfall eines Endgerätes dazu führt, dass die gesamte Netzkommunikation unterbrochen wird (Ausnahme bei Protection-Umschaltung - siehe: FDDI). Das stimmt bei neuen Karten allerdings nicht mehr, da jede Karte diese Protection-Umschaltung beherrscht. Andererseits gibt es wenig Alternativwege, was im Falle von hohen Lastzuständen auf einem Ringabschnitt zu Engpässen führen kann.
- Teure Komponenten
- Darf/kann nicht für kombinierte Rechnernetz-/Telefonverkabelung eingesetzt werden
- relativ hoher Durchmesser, d.h. hohe Latenzen zu entfernten Knoten
- Hoher Verkabelungsaufwand

Beispiele:

- Token Ring (logisch)

- FDDI (physisch)

In der Theorie sieht man oft, dass die physikalische Ringstruktur dem logischen Aufbau folgt, um Leitungslängen und damit Kosten zu sparen. Dies geschieht jedoch in der Regel auf Kosten der Flexibilität bei Erweiterungen.

Bus-Topologie

Eine Bus-Topologie (Linien- oder Strangtopologie) besteht aus einem Hauptkabel, dem Bus, an das alle Geräte und zwei Endwiderstände angeschlossen sind. Diese Abschlusswiderstände mit dem Leitungswellenwiderstand (Z = 50 Ohm bei Koaxialkabel) dienen zu Verhinderung von Reflexionen. Der Anschluss zwischen den Geräten (also Netzkarten) und Hauptkabel erfolgt über T-Stücke.

Zugriffsverfahren (z. B. CSMA/CD) versuchen zu verhindern, dass sich die Teilnehmer gegenseitig stören. Sie regeln, welcher Teilnehmer die gemeinsame Leitung – den Bus – zu welchem Zeitpunkt zur Verfügung hat.

Bei diesem Verfahren treten folgende Probleme auf:

Während des Datenverkehrs muss jeder Teilnehmer jede Sendung mithören. Dadurch steigt die Belastung (Strom) der Ausgangsbaugruppen des Senders mit der Anzahl der Teilnehmer am Bus.

Kollisionen können vermieden werden, allerdings nicht bei Verwendung von CSMA/CD + Ethernet. Dies ist bei Feldbussystemen möglich, z. B. bei einem CAN-Bus mit CSMA/CA.

Feldbussysteme können sich über einen Bereich von mehreren hundert Metern erstrecken. Hier ist die Leitungslänge im Vergleich mit der Wellenlänge der Übertragung nicht mehr vernachlässigbar klein. Um störende Reflexionen zu vermeiden, werden Busabschlusswiderstände benötigt, die die Ausgänge des Senders ebenfalls mit höheren Strömen belasten. Kleinere Feldbussysteme können dennoch sehr gut nach dem Bus-Prinzip vernetzt werden.

Die Daten können in beide Richtungen übertragen werden. Vorteile eines Busnetzes sind der geringe Kabelbedarf und die Unabhängigkeit von der Funktion einzelner Stationen: Bei einem Ausfall eines Knoten oder einer Station bleibt das gesamte System trotzdem intakt. Größte Gefahr ist jedoch ein Kabelbruch im Hauptkabel durch den der ganze Bus ausfällt.

Die Bus-Topologie ist eine passive Topologie, d.h. die angeschlossenen Stationen führen keine Wiederaufbereitung des Signals durch. Sie greifen die Signale vom Kabel ab oder senden auf das Kabel wo sich das Signal dann in beide Richtungen ausbreitet. Hier wird von einem Diffusionsnetz gesprochen.

Vorteile:

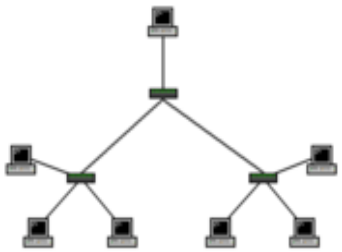
- Der Ausfall eines Rechners hat keine Konsequenzen
- Nur geringe Kosten, da nur geringe Kabelmengen erforderlich sind
- Einfache Verkabelung und Netzerweiterung
- Es werden keine weiteren Rechner zur Übermittlung der Daten benötigt

Nachteile:

- Alle Daten werden über ein einziges Kabel übertragen.
- Datenübertragungen können leicht abgehört werden (Stichwort: Sniffer).
- Eine Störung des Übertragungsmediums an einer einzigen Stelle im Bus (defektes Kabel) blockiert den gesamten Netzstrang.
- Es kann immer nur eine Station Daten senden. Während der Sendung sind alle anderen blockiert (Datenstau).
- Aufgrund der Möglichkeit der Kollisionen sollte das Medium nur zu ca. 30 % ausgelastet werden.

Baum-Topologie

Baum-Topologien sind dadurch gekennzeichnet, dass sie eine Wurzel (der erste bzw. obere Knoten) haben, von der eine oder mehrere Kanten (Links) ausgehen. Diese führen weiterhin zu einem Blatt (Endknoten) oder rekursiv zu Wurzeln weiterer Bäume.



Technisch gesehen ist die Baum-Topologie eine Netz-Topologie, bei der mehrere Netze der Stern-Topologie hierarchisch miteinander verbunden sind. Hierbei müssen Verbindungen zwischen den Verteilern (Hub, Switch) mittels eines Uplinks hergestellt werden. Häufig wird diese Topologie in großen Gebäuden eingesetzt.

Vorteile:

- Der Ausfall eines Endgeräts hat keine Konsequenzen.
- Strukturelle Erweiterbarkeit,
- Große Entfernungen realisierbar (Kombination),
- Gute Eignung für Such- und Sortieralgorithmen.

Nachteile:

- Bei Ausfall eines Verteilers (Wurzel) ist der ganze davon ausgehende (Unter)Baum des Verteilers "tot".
- Zur Wurzel hin kann es bedingt durch die für Bäume definierte Bisektionsweite von 1 zu Engpässen kommen, da zur Kommunikation von der einen unteren Baumhälfte in die andere Hälfte immer über die Wurzel gegangen werden muss.
- Bäume haben mit zunehmender Tiefe (=Anzahl der zu gehenden Links von der Wurzel bis zu einem Blatt) einen sehr hohen Durchmesser. Dies führt in Verbindung mit der Bisektionsweite zu schlechten Latenzeigenschaften bei klassischen Bäumen.
- Um diesen doch recht gravierenden Nachteilen entgegenzuwirken, wird in der Praxis eine Vielzahl von Baumvariationen verwendet, die jedoch hier nicht weiter erwähnt werden.

Anhang 8: Literatur- und Quellenangaben

- Scagliola,B.: Ergonomie und Olivetti, Buch 1 und 2, Olivetti 1981
- Berliner Informationsgesetzbuch
  - Teil 1 Datenschutzgesetze
  - Heft 1 - Berliner Datenschutzgesetz (mit Informationsverarbeitungsgesetz IVG)
  - Heft 2 – Bundesdatenschutzgesetz
  - Scheckheft zum Datenschutz
- Tischer, Michael: PC intern 4, Data Becker GmbH & Co. KG, 1. Auflage 1994
- Dr. Helmut Bähring: Mikrorechner-Systeme, Springer-Verlag Berlin Heidelberg, 1991
- Messmer, Hans-Peter: The Indispensable PC Hardware Book, Addison-Wesley Publishing Company, 1993
- Mueller, Scott: PC-Werkstatt, Addison-Wesley GmbH,1. Auflage 1992
- Oerter, Joachim Gebhard: Feichtinger, Herwig, Arbeitsbuch PC Hardware, Franzisverlag,2. Auflage 1992
- ”Bildschirmarbeit human gestalten”. Hrsg.: DGB Technologie Beratung e. V. Berlin, Kleiststr. 19 - 21, 10787 Berlin
- Berliner Datenschutzgesetz
- Tarifvertrag über den Einsatz von Geräten der Informationstechnik in der Berliner Verwaltung
- Richtlinie der Europäischen Union 90/270 EWG
- Wikipedia
- Schulungsunterlagen der Firma Herdt
- IT-Nachrichten für die Berliner Verwaltung („Splitter“) Ausgabe1/2008

Interessante Internetseiten

- www.klicksafe.de
- www2.tu-berlin.de/www/software/hoax.shtml
- www.bsi-fuer-buerger.de

Anhang 9: Probeklausur

Bearbeitungshinweise :

Jedes Blatt, ist rechts oben mit Ihrem Namen zu kennzeichnen. Lassen Sie auf der rechten Seite eines jeden Blattes einen Korrekturrand von 4 cm. Lesen Sie vor der Beantwortung einer Aufgabe die Fragestellung genau durch.

Sachverhalt:

Als neue Dienstkraft in der Abteilung I Ihrer Behörde werden Sie freundlich begrüßt.
Ihr Vorgesetzter, der Referatsleiter Herr Müller, hatte Sie speziell für den Einsatz im IT-Bereich für sein Referat angefordert.

Nach einem kurzen Einführungsgespräch in Ihre zukünftigen Aufgaben, bittet Sie Herr Müller, dem bei ihm sitzenden Anwärter einige allgemeine Fragen zur Informationstechnik zu beantworten, da er leider mit Terminen überhäuft sei.

1. Erklären Sie kurz die Ihnen bekannten Ziele für den Einsatz von Informationstechnik (6 Punkte)
2. Welche Informationsarten gibt es? Nennen Sie die unterschiedlichen Formen! (4 Punkte)
3. Wie lautet das Grundprinzip der Datenverarbeitung? Erklären Sie anhand einer Zuordnung von je zwei Hardwarekomponenten dieses Grundprinzip. (8 Punkte)
4. Welche Aufgaben hat ein Betriebssystem? (4 Punkte)
5. Wie werden Laufwerke unter dem BS bezeichnet – angesprochen? (2 Punkte)
6. Was ist eine Datei? (3 Punkte)
7. Nennen Sie die Elemente der Benutzeroberfläche. (5 Punkte)
8. Wofür benötigen Sie RAM in Ihrem Computer? (2 Punkte)
9. Was ist unter dem Begriff Windows zu verstehen? (4 Punkte)
10. Begründen Sie die Vorteile einer einheitlichen Benutzeroberfläche! (2 Punkte)

Sachverhalt:

Aufgrund Ihrer Empfehlungen wurde für die PCs der Sachbearbeiter Word für Windows beschafft.

Leider arbeiten Ihre Kollegen bislang sehr uneffektiv mit dem vorhandenen PC-Textverarbeitungsprogramm - Word. Es kommt oft zu Überspeicherungen (Dateien werden mit anderen Dateien überschrieben) und anderen Pannen.

Außerdem hat Herr Müller gehört, dass durchschnittliche Anwender nur bis zu 20 % der Fähigkeiten eines Textverarbeitungsprogramms tatsächlich ausnutzen. Insbesondere die

Fertigung von Serienbriefen und der Einsatz von Autotext (Textbausteinen) interessiert Ihren Referatsleiter.

Herr Müller möchte den Umgang all seiner Mitarbeiter mit dem Programm optimieren. Seine Arbeitsaufträge an Sie lauten deshalb:

11. Zählen Sie 8 wichtige Funktionen eines Textverarbeitungsprogramms (neben der Erstellung von Serienbriefen) auf.
    (4 Punkte)
12. Erklären Sie, was ein Serienbrief ist. Vergleichen Sie dazu die Verwendung von Serienbriefen mit dem dazugehörigen herkömmlichen Verfahren und nennen Sie die Vorteile der Serienbriefmethode
    (6 Punkte)
13. Nennen Sie den Unterschied zwischen Textverarbeitung und Textbearbeitung?
    (4 Punkte)
14. Wo findet die Funktion Autokorrektur ihre Anwendung?
    (2 Punkte)

Sachverhalt:

Aufgrund der häufigen Preissenkungen bei Hardwarekomponenten versuchen Ihre Kollegen durch häufige Berechnungen immer den günstigsten Einkaufspreis für aktuelle Beschaffungen zu erzielen. Da dies sehr zeitaufwendig ist, werden Sie mit der Arbeit betraut.

15. Welche Software würden Sie einsetzen? Begründen Sie bitte Ihre Entscheidung, indem Sie die Vorteile der Software gegenüber einem Taschenrechner aufzeigen.
    (4 Punkte)

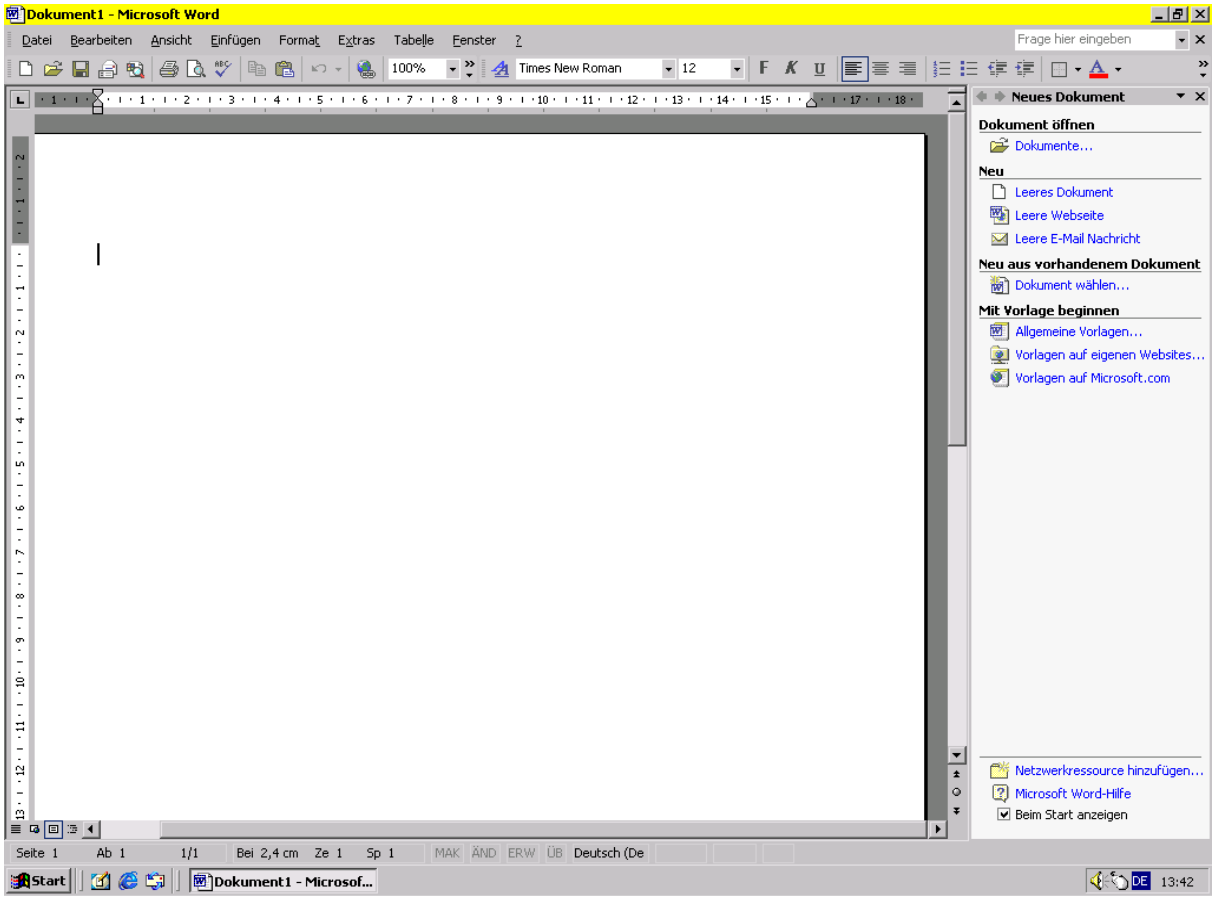
Sachverhalt:

Bei Ihrer Tätigkeit in der neuen Dienststelle fällt Ihnen immer wieder auf, dass Sie und Ihre Kollegen bei der Beschreibung von Problemen und deren Lösungen oft aneinander vorbei reden. Der wohl wichtigste Grund ist die Verwendung verschiedener Fachausdrücke und Möglichkeiten Befehle zu wählen.

16. In der Hoffnung diese Kommunikationsschwierigkeiten in Zukunft zu vermeiden, soll folgende Grafik von Ihnen beschriftet werden, um dann an die Kollegen ausgegeben zu werden.

    Ordnen Sie die folgenden Begriffe zu:
    (8 Punkte)

Titelleiste	Cursor
Statuszeile	Aufgabenbereich
Bildlauffeld	Symbolleiste
Ansichtensteuerung	Menüzeile



Sachverhalt:

In einer kurzen Pause werden Sie von einem neuen Mitarbeiter nach einigen für Ihn unklaren Punkten befragt. Versuchen Sie Ihrem Kollegen zu antworten.

17. Welche Gründe gibt es für den Einsatz von Netzwerken? Nennen Sie 6 Gründe!
    (6 Punkte)
18. Was ist ein Intranet?
    (1 Punkt)
19. Seit wann gibt es Computerviren?
    (2 Punkte)
20. Was ist ein Computervirus?
    (6 Punkte)
21. Nennen Sie 6 Komponenten bei der Betrachtung eines ergonomischen Arbeitsplatzes, mit einer kleinen Beschreibung, welche Aspekte beachtet werden!
    (3 Punkte)

Anhang 10: Lehrpläne

Lehrplan für den Ausbildungsberuf **Fachangestellte/r für Bürokommunikation**

Fachgebiet: Einführung in die Anwendung der Informationstechnik (IT)	**58 DS**[19]
Allgemeine Grundlagen	3 DS
Aufbau der IT sowie das Zusammenwirken der Komponenten	5 DS
Umgang mit Anwendungen der IT	41 DS
Organisatorische und rechtliche Regelungen	1 DS
Auswirkungen der IT/Ergonomie	3 DS
Leistungsnachweis	5 DS

Lehrplan für die/den **Verwaltungsfachangestellte/n**

Fachgebiet: Einführung in die Anwendung der Informationstechnik (IT)	**20 DS**
Allgemeine Grundlagen	4 DS
Aufbau der IT sowie das Zusammenwirken der Komponenten	1 DS
Umgang mit Anwendungen der IT	11 DS
Organisatorische und rechtliche Regelungen	1 DS
Auswirkungen der IT/Ergonomie	1 DS
Leistungsnachweis	2 DS

Lehrplan für den **Verwaltungslehrgang I für Angestellte**

Fachgebiet: Einführung in die Anwendung der Informationstechnik (IT)	**18 DS**
Allgemeine Grundlagen	3 DS
Aufbau der IT sowie das Zusammenwirken der Komponenten	1 DS
Umgang mit Anwendungen der IT	9 DS
Organisatorische und rechtliche Regelungen	2 DS
Auswirkungen der IT/Ergonomie	2 DS
Leistungsnachweis	1 DS

[19] DS = Doppelstunde

Die Inhalte und Schwerpunkte variieren unter den oben aufgeführten Ausbildungsgängen. Daher können an dieser Stelle die genauen Stundenansätze nicht genau wieder gegeben werden. Es wurde versucht, eine Vergleichbarkeit in Bezug auf die Themen herzustellen. Für die Ausbildung sind die individuellen Lehrpläne maßgebend.

gegründet 1919